OECD publishing

TRANSPARENCY REPORTING

CONSIDERATIONS FOR THE REVIEW OF THE PRIVACY GUIDELINES

OECD DIGITAL ECONOMY PAPERS

April 2021 **No. 309**

OECD
BETTER POLICIES FOR BETTER LIVES

Foreword

This report aims to review transparency reporting practices in the context of government requests for access to personal data held by the private sector. The report serves to inform and guide further discussions amongst members of the OECD Working Party on Data Governance and Privacy in the Digital Economy (DGP), the Privacy Guidelines Expert Group, and the Secretariat as part of the review of the implementation of the OECD Privacy Guidelines [OECD/LEGAL/0188].

This paper was drafted by Dr José Tomás Llanos, Research Fellow, Department of Science, Technology, Engineering and Public Policy (STEaPP), University College London (UCL), London, United Kingdom, with input from Elettra Ronchi and Lauren Bourke of the OECD Secretariat. The author is grateful for the feedback received from the expert group established to support the review of the OECD Privacy Guidelines and delegates of the Working Party on Data Governance and Privacy. The paper was further discussed at the virtual OECD Expert Roundtable on "Data localisation and Trusted Government Access to Data" held on 5-6 October 2020. The work was made possible by the generous contributions of Japan.

Note to Delegations:

This document is also available on O.N.E under the reference code:

DSTI/CDEP/DGP(2020)8/FINAL

DSTI/CDEP/DGP(2020)8-ANN/FINAL

Table of contents

Executive Summary

The Internet has opened multiple avenues for individuals to communicate, express their opinions, access information about a myriad of topics, and purchase goods and services. During these interactions with the digital environment, individuals generate different types of data, oftentimes revealing private aspects of their lives. That data can be of high value to governments engaging in auditing, intelligence gathering, fulfilling their law enforcement duties, or seeking to protect their citizens and perform their functions more efficiently.

Government demands (or requests) to gain access to this data have grown significantly in the past decades. The practices and due process rules regarding targeted data access requests (e.g. in relation to a specific user, account or phone number) have been relatively clear for some time. However, practices and processes regarding bulk access requests (i.e. requests for access to large quantities of data, typically for intelligence and national security purposes) are typically less transparent, thereby raising important civil liberties and privacy concerns which can cause distrust in the digital economy and hamper the transborder flow of data.

Media coverage and empirical research on state surveillance have confirmed that governments have been accessing with relative ease large amounts of user data held by private entities. To provide more clarity regarding the extent to which government are accessing user data, and wary of possible erosion of consumer trust, since 2010 some companies have started to issue transparency reports in this connection. The ad hoc growth of voluntary transparency reporting, however, has resulted in the publication of reports with varying degrees of granularity, dissimilar metrics and diverse terminology.

Findings in this report

This report compares the transparency reports of 20 of the most widely used online content-sharing services in OECD countries in order to determine whether current transparency reporting practices allow an assessment of the extent to which governments are gaining access to privately-held data, as well as whether the information provided is useful and comparable. This analysis has led to the following findings:

1. The surveyed companies' reporting approaches vary significantly. Except for broad metrics (e.g. total number of government requests and number of requests where some information was produced), most reported data cannot be compared. As a consequence, drawing a sector-wide 'big picture' is difficult, as the informative value of the available data is highly limited.
2. Partly due to restrictions to transparency reporting imposed by law, current transparency reporting practices do little to allay existing concerns regarding unlimited or bulk access to user data by governments that arise in the context of national security and foreign intelligence investigations.

3. The reporting of specific figures about cases where the users specified in the requests were notified prior to the production and surrendering of information can be a valuable tool to increase trust and transparency. Yet, this metric is seldom reported.
4. There is no industry-wide standard for the frequency with which companies should publish transparency reports. The absence of a standard publication schedule means that transparency reports cannot be easily compared, which impinges on their informative value.
5. Overall, given the surveyed companies' different reporting approaches, including on metrics and terminology, transparency reporting is in urgent need of guidelines and minimum standards to provide in the aggregate reliable information on the extent to which governments are gaining access to user data held by the private sector.

Good practices in transparency reporting

A number of good practices in transparency reporting were identified which, if implemented widely by reporting entities, would significantly enhance transparency and improve the comparability of the reported data.

When it comes to transparency reporting, the more granularity, the better. It is the view of the author that companies should structure the reports to include, at a minimum, the number of requests they receive over a clearly delineated time period, differentiating between each type of legal process and/or category of request (e.g. warrant, subpoena, emergency request). To the extent possible, companies should also report their responses to government requests for each type of process or request category, disclosing the number, or at least the percentage, of subjects (i.e. account, user or other identifier) impacted by the request. It is important, however, to keep in mind that for many companies, the biggest barrier for engaging with transparency reporting is operational. Reporting schemes are onerous, and may not be viewed by companies as ultimately being worth it. A balance must therefore be found between a standardised comprehensive reporting system and one that is not too costly.

Proposed next steps

Governments should work and liaise with companies, data protection authorities, international organisations and civil society organisations to develop meaningful guidance for transparency reporting (including harmonising terminology use) in order to improve the potential for comparisons to be made across companies, sectors and jurisdictions.

This report focuses on some of the largest Internet companies in the world, many of which are based in the United States. More research should be carried out on companies based elsewhere, ideally on a per country basis, with an aim to both identify similarities and disparities concerning transparency reporting across different countries' applicable laws and build a robust evidence base required to agree on minimum common standards and guidance on good practices that are reliable and comparable on a both national and international level. Relatedly, to elucidate the extent to which different governments are gaining access to user data held by the private sector, transparency reporting by governments should be encouraged and widely adopted.

More work should also be done to understand transparency reporting practices by the providers of telecommunications service providers, given the frequency with which they are subject to specific information access/disclosure requests and obligations.

Lastly, governments should engage with companies, data protection authorities, international governmental organisations, civil society organisations, and other regulatory bodies (including those in

charge of administrative simplification), to debate on, encourage and ultimately facilitate the removal or at least reduction of unnecessary and disproportionate legal barriers to transparency reporting. The input from both governments (especially those with open government initiatives) and companies as to what they consider an unnecessary and disproportionate barrier should assist the execution of this task.

Introduction

Governments routinely need access to user/consumer data held by private entities in order to perform public functions. A traditional example is an audit of a company's records to verify that the correct tax has been paid. Numerous laws in multiple jurisdictions have been enacted in the last decades granting law enforcement authorities greater access to companies' information. The growth in government demands for companies' records and personal data about users, and particularly the scale and scope of bulk access by governments, has, however, been a reason for concern. One response to this situation has been an effort by companies to shed light on government requests for user data through the publication of transparency reports.

Transparency reporting is useful for promoting trust in organisations with substantial holdings of personal data, and contributes to demonstrate that they are accountable in their information handling practices. Transparency reporting may also be seen as a social compact under which citizens expect their communications and affairs to be maintained in confidence, subject only to lawful and proportionate law enforcement and national security exceptions, with the relevant organisations subject to trustworthy independent oversight.

Transparency reporting, however, serves purposes that go beyond trust promotion and accountability. Indeed, transparency makes 'processes of governance and lawmaking as accessible and as comprehensible as possible' (Birkinshow, 2006, pp. 189-190), striking a balance between the provision of information about state activities to the public and not encumbering states' ability to protect their citizens and perform their functions.

As it is not generally a legal obligation to release transparency reports, the ad hoc growth of voluntary company transparency reporting on government access to personal data has resulted in the reporting of multiple statistics, metrics and numbers that are not always comparable with each other, such as the subject of the requests (e.g. accounts requested, users specified, URLs affected) and the outcome of the requests (e.g. percentage of requests where some data was produced vs percentage of requests where all or some data was produced). Lack of standardisation in the reporting of government requests for user data undermines companies' efforts to elucidate the magnitude of states' access to individuals' private information, the regularity at which such requests are made, the legal bases relied upon to gain that access, and the available options, if any, that users have at their disposal to be informed on governments' requests to access data about them.

Fostering trust in the digital economy through improved transparency is a long-standing OECD objective. The "openness" principle of the OECD Privacy Guidelines dates back to the original 1980 adoption and counsels in favour of a general policy of openness about the processing of personal data [OECD/LEGAL/0188]. The 2011 OECD Recommendation on Principles for Internet Policy Making (IPPs) also calls for policies that ensure transparency, fair process and accountability. It recognises that policy making for the Internet should promote openness and be grounded in respect for human rights and the rule of law (OECD, 2011). Similarly, the 2016 OECD Ministerial Declaration on the Digital Economy (the

'Cancún Declaration') features a commitment to reinforce the Internet's openness, while respecting applicable frameworks for privacy and data protection (OECD, 2016).

This report (the 'Report') aims to contribute to the current review of the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data [OECD/LEGAL/0188], in particular in connection with concerns of potentially unlimited government access to personal data held by the private sector. The findings of this Report may serve to identify actions that could be undertaken to encourage regular and comparable transparency reporting on government demands for user data, including personal data, with an aim to promote trust in the digital economy, enhance private companies' accountability and protect individuals' fundamental rights and freedoms, especially the rights to privacy and data protection. To this end, this Report documents current practices in transparency reporting on government demands for user data by a sample of 20 Internet-based companies (the 'Companies'), and on the basis of this information, it identifies commonalities and trends, offers insights and highlights good practices capable of improving comparability amongst transparency reports, and by extension their informative value.

An important objective of this Report is to determine whether the Companies' transparency reports allow the reader to identify the number and nature of government requests for user data, the number of subjects of the requests (e.g. number of users, accounts or other identifiers to which those requests relate), the outcome of the request (i.e. the Company's actions in response to the request), the volume of accessed information or affected individuals, the terminology the Companies use and the types of requests they receive (i.e. the legal form of the request such as a judicial warrant or an administrative request). In addition, other aspects such as the Companies' policy on providing notice to users prior to the disclosure of information and notable reporting practices are also surveyed.[1]

The sample of Companies include some of the world's most widely used[2] social media platforms, online communications services, file sharing platforms, and other online services that enable the uploading, posting, sharing and/or transfer of digital content and/or facilitate voice, video, messaging or other types of online communications. A list of the Companies in alphabetical order appears in Annex A. These Companies were chosen based on their popularity, their ability to collect, hold and process large volumes of data, and the fact that they currently issue or have issued transparency reports on government requests for user data. The latter fact was ascertained during the preparation of the Benchmarking Report on Transparency Reporting on Terrorist and Violent Extremist Content (TVEC) (internal document), which involved an examination of the world's top 50 online content-sharing services' transparency reporting practices concerning TVEC. Thus, the work presented in this Report leverages previous research carried out in the context of the aforementioned Benchmarking Report.

After the Companies were selected, a standardised profile template was devised, addressing all the fields of information that comprise the scope of the research, as summarised earlier. One profile per Company was developed based on each Company's transparency reports published to date. The Companies' profiles, which appear in Annex C, are the evidence base from which the findings of this Report were derived. It must be stressed that, as the sample of Companies is composed of online content-sharing services only, it may not be fully representative of all industry segments that are of relevance to determine the extent to which governments are gaining access to data held by the private sector. In addition, on account of the selection criteria, the majority of the Companies in the sample (17 out of 20) are US-based. **To build a more comprehensive evidence base, future work should include telecommunications service providers, as well as more companies based in jurisdictions other than the United States (see further Section 4 below).**

The focus of this Report is transparency reports by private companies. However, whilst companies have the responsibility to respect the privacy of their users and to respond to their stakeholders' concerns, the primary duty to protect the right to privacy - and associated rights and fundamental freedoms – is

incumbent upon governments. Accordingly, if there is concern about how government agencies are using their surveillance powers, governments are in the best position to explain how they are using those powers. In this regard, the United Kingdom and United States have published periodic reports on the use and exercise of national security authorities and investigatory powers, including statistics on the types and volumes of user data they accessed during the reporting period.[3] More governments should ideally follow suit, thus responding to calls to increase transparency in a more effective fashion.

This Report is structured as follows. Section 1 presents some background on transparency reporting. Section 2 provides an objective snapshot of the Companies' current practices concerning transparency reporting on government requests for user data, identifying a number of commonalities and trends. Also, this section offers a number of insights about the informative value of the Companies' reported data and specific areas of transparency reporting in need of improvement. Section 3 highlights good practices in transparency reporting that reporting entities should implement as minimum standards to enhance comparability amongst the reported data. Section 4 sets out a number of recommendations for next steps.

1. Background on transparency reporting

It is axiomatic that reliable, comprehensive information is essential for understanding any given problem and the progress being made towards its solution. Such information is also necessary to inform debate and productive deliberation. Transparency reporting has emerged in different areas[4] to serve these and related ends. Government requests for user data held by private companies is a case in point. The Internet has opened multiple avenues for individuals to communicate, express their opinions, views and beliefs, access information about myriad topics and purchase goods and services. During these interactions in the digital environment, individuals generate different types of data, oftentimes revealing private aspects of their lives. Internet-based companies typically collect, store and process such user data to provide and improve their services, and more generally to engage in data-driven innovation. That data is typically of high value to governments engaging in intelligence gathering, fulfilling their law enforcement duties, or seeking to protect their citizens and perform their functions more efficiently. Given the large user data troves that some online companies amass, governments across the globe have been increasingly targeting these companies with demands to gain access to their users' data.

Concerns about governments' access to data held by the private sector

There is a fundamental distinction between scenarios where government officials demand from private entities data concerning a particular target (e.g. a specific user, account or phone number), and on the other hand, scenarios where the government is accessing large quantities of data without discrimination (i.e. bulk access). For targeted requests, which normally relate to law enforcement investigations, relevant practices and due process rules tend to be relatively clear. When seeking data about an individual in a criminal investigation, a particular threshold of suspicion that links the individual to a specific crime must be met; independent authorisation for the surveillance or data access must be obtained (e.g. in the form of a warrant); and the intrusion into privacy must be limited in time and scope to the acquisition of evidence relevant to the crime under investigation (Cate and Dempsey, 2017a).[5]

However, new paradigms seemed to have emerged in relation to state powers. The leakage of classified documents by former US National Security Agency (NSA) Edward Snowden in 2013 revealed a number of surveillance activities carried out by the US and the UK governments which involved bulk, ongoing and sometimes real-time access to phone and Internet metadata, as well as to the content of communications (Rubinstein, Nojeim and Lee, 2014, pp. 100-102). It is now clear that governments have been collecting data without specific suspicions concerning a crime, typically for intelligence and national security purposes.[6] These demands for bulk access to privately-held datasets by governments raise important civil liberties and privacy concerns which warrant careful attention.

To be sure, concerns about government requests for access to data held by the private sector predate the revelations by Edward Snowden in 2013. However, said revelations called into question the handling of personal data by major US telecom and Internet-based companies, causing a consumer trust crisis to which companies responded by publishing detailed reports about government demands for data (New America, 2017). There is little doubt today that Internet businesses with large data holdings about

individuals are under market pressure to be much more open about the manner in which they respond to governments' requests for access to said data.

Not only are individuals and privacy advocates concerned about the growth in government demands for companies' private information; companies themselves have complained about this trend, typically from the point of view of compliance costs, which may be substantial. In addition, companies are caught in the middle between competing interests, as they face the difficulty of reconciling the release of confidential personal data to government authorities with the relationship of trust they seek to maintain with their customers (Gidari, 2007, p. 535). There are also concerns about legal liability when companies are subject to competing legal responsibilities to protect security and confidentiality and also comply with access requests from state authorities in a particular jurisdiction (International Working Group on Data Protection in Telecommunications, 2015). Legal challenges are compounded where a corporate holding operates in several jurisdictions and there is a conflict of laws, or where a processor member of the holding is requested to covertly release the data of another firm belonging to the same group. There are additional difficulties in the context of cross-border requests under Mutual Legal Assistance Treaties (MLAT).[7]

Law enforcement and national security legislation often includes restrictions preventing businesses from disclosing information relating to government user data access demands, barring even the disclosure of aggregate statistics. In many countries, commercial operators are also prohibited from providing the public with any insight into the manner in which they respond to those requests. These restrictions can make it difficult for companies to respond to public demand for greater transparency. The result is an increasing flow of data from businesses to government that is largely opaque to the customers and citizens whose data is at issue.

Calls for greater transparency regarding government access

Concerns about the lack of transparency regarding government demands for data held by private companies are widely shared. In 2014, a report of the United Nations High Commissioner for Human Rights highlighted "the disturbing lack of governmental transparency associated with surveillance policies, laws and practices, which hinders any effort to assess their coherence with international human rights law and to ensure accountability" (Office of the United Nations High Commissioner for Human Rights, 2014). The Global Network Initiative (GNI) has, since its launch in 2008, advocated for greater transparency regarding government access to user data,[8] and many individual companies have made public their frustration with the current limitations in what they can say about the requests made and their responses.[9] In 2013, a civil society coalition put forward principles on human rights and surveillance that call for greater transparency by governments themselves about access requests as well as for non-interference by governments in efforts by companies at public reporting in this area (Access Now, EFF et. al., 2014). Also in 2013, a group of Internet businesses and civil society groups urged for greater transparency around national security-related requests to Internet, telephone, and web-based service providers for information about their users and subscribers (Center for Democracy and Technology, 2013). The Telecommunications Industry Dialogue on Freedom of Expression and Privacy issued in 2013 Guiding Principles that call on companies to produce annual reports on their efforts to protect free expression and privacy in the context of government access requests. In 2017, each of the companies participating in the Telecommunications Industry Dialogue (including AT&T, Nokia, Orange and Telefónica) reported publicly on their implementation of the Guiding Principles in practice (Telecommunications Industry Dialogue, 2017, p. 6). In 2016, the Transparency Reporting Toolkit, a project by New America's Open Technology Institute (OTI) and Harvard University's Berkman Center for Internet & Society, issued a report identifying best practices, establishing reporting guidelines, and providing a transparency report template, with a view to improve and harmonise transparency reporting on government requests for privately-held data (Woolery, Budish and

Bankston, 2016, pp. 104-105). The US government too has acknowledged the need for greater transparency in this area.[10]

In 2011, The Privacy Projects (TPP) began to study the issues surrounding systematic government access to user data through a series of expert reports and roundtable discussions. One of the key findings from that work is the existence of a serious transparency gap surrounding both the laws as well as governmental agency practices (Box 1).

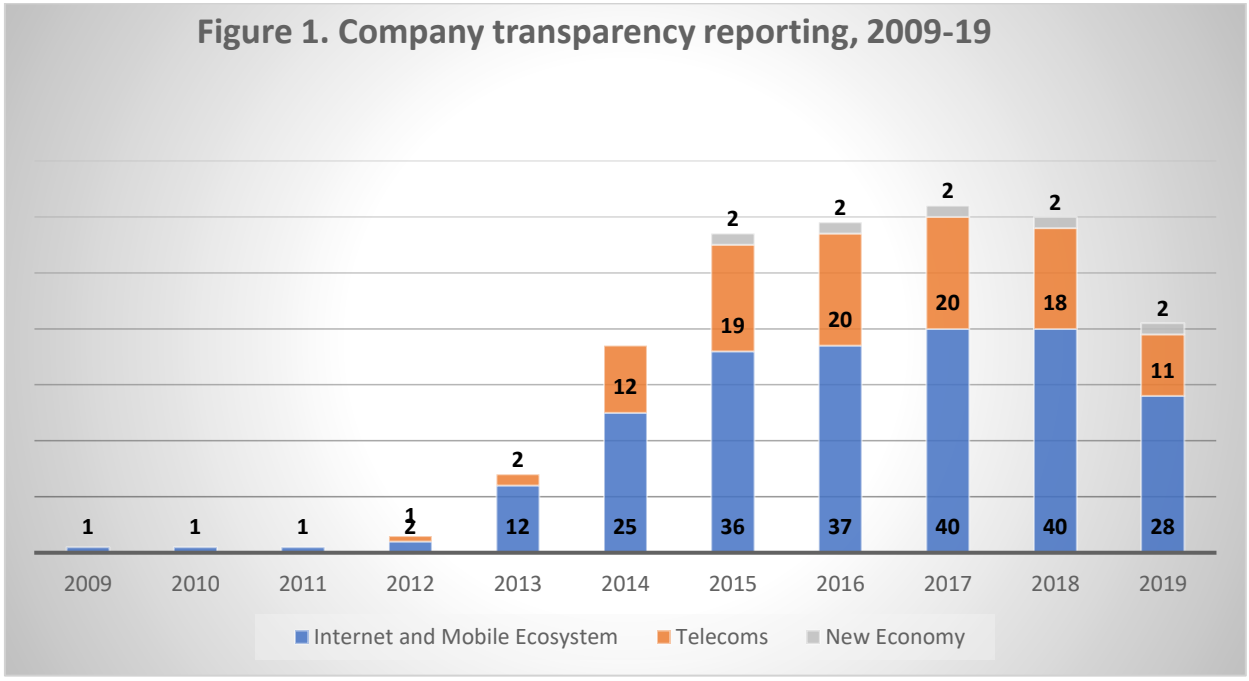
Box 1. Findings from TPP work

- Systematic access demands do appear to be growing, although the recent (i.e. Snowden) disclosures make it clear that governments are not only demanding stored data in bulk, but also are tapping into cables to collect or filter large swaths of data as it moves across the Internet.
- There is a profound lack of transparency about countries' laws and practices. Relevant laws are at best vague, and government interpretations of them are often hidden, especially in the national security realm.
- In particular, published laws and policies do not expressly address the unique challenges of bulk collection.
- Plummeting data storage costs and enhanced analytical capabilities spur governments' appetites to collect more data.
- As Internet-based services have become globalised, surveillance has become trans-border, posing increased legal and reputational risks to businesses operating globally.

Source: Kuner, C., Cate, F., Millard, C. and Svantesson, D.J.B., "Systematic Government Access to Private-Sector Data Redux" (2014) 4 *International Data Privacy Law* 1 and country surveys within the International Data Privacy Law Journal symposium issues ((2014) 4/1 and (2012) 2/4).

Releasing privately-held information to a third party for a non-business purpose, without consent from the individuals concerned and probably contrary to their wishes and preferences, is problematic from a privacy standpoint. In law enforcement cases, this tension has been resolved by recognising law enforcement investigations as a legitimate exception to non-disclosure expectations. However, a continuing and pressing concern that remains since the Snowden revelations is the potential growth in access by governments to privately-held information as a routine rather than exceptional investigative technique, and to the bulk release and real-time access to said information for surveillance purposes (International Working Group on Data Protection in Telecommunications, 2015, p. 7).

One response to the abovementioned challenges of traditional data protection expectations has been to demand that both public entities and private companies demonstrate that they are responsible in and accountable for their data handling practices. Companies found a way to do this through the publication of transparency reports. Google published its first transparency report in 2009 followed by a handful of telecommunications and internet services companies in the next 3 years. However, the practice really took off in 2013 with dozens of companies publishing transparency reports in North America, Europe, Asia and Australasia. Since the release of Google's first report in 2009, by 2019 more than 70 companies had issued public reports, according to the Transparency Reporting Index.[11] Figure 1 below presents the number of companies that have issued transparency reports in the period 2009-2019, broken down by three industry segments (Internet and mobile ecosystem, telecoms and new economy).



Source: OECD based on data from the Transparency Reporting Index. https://www.accessnow.org/transparency-reporting-index/ [accessed June 2020]

These reports represent an important step forward in increasing the transparency associated with government access to private companies' user data. Although transparency reporting has flourished in recent years and different companies have experimented with innovative and new approaches to reporting, the practice has also suffered from a lack of consistency that has limited the reports' usefulness. Due to different accounting and reporting practices, and a lack of clarity about exactly how companies are counting or defining certain terms, it is difficult to compare and analyse data across companies.

As a result, there have been growing calls for improving the quality and comparability of companies' transparency reports, as well as for identifying unnecessary barriers to making these improvements. Against this background, this Report surveys the transparency reports published to date by the Companies listed in Annex A. This exercise is carried out with an aim to document current practices in transparency reporting on government requests for Internet-based companies' user data, and determine whether said practices allow readers of transparency reports to identify the number and nature of government requests for user data, with what frequency they do so, the volume of data they access based on these requests, the type of data they seek, the processes they follow to this end and other associated aspects of transparency reporting. The findings of this Report can serve to identify areas in transparency reporting in need of improvement, as well as reporting approaches and good practices that facilitate comparability and enhance the informative value of transparency reports in general.

2. Objective snapshot, trends and insights regarding the Companies' transparency reporting

This Section sets forth the state of play amongst the Companies' current practices relating to transparency reporting on government requests for user data, presenting firstly an objective snapshot thereof and then identifying trends and offering insights concerning six main aspects: nature and number of the requests, outcome of the requests, indication of the legal processes required to access different types of information / explanation of international requests processing, reporting on user notifications, reporting on the services targeted by the requests, and the frequency with which transparency reports are issued.

Generally, the Companies' reporting approaches in most of the aforementioned areas vary significantly. As a consequence, except for broad metrics such as the total number of government requests received and the number of requests where some information was produced (i.e. outcome of the requests), most reported data cannot be compared across the surveyed Companies. Therefore, that data's informative value to draw a sector-wide (i.e. encompassing all the Companies) 'big picture' is highly limited.

Given the Companies' different reporting approaches and a lack of clarity about exactly how they count some metrics and define certain terms, transparency reporting on government requests for user data is in urgent need of standardisation to enable truly informative industry- or sector-wide analyses. Only with more uniform and granular reporting, following at a minimum the good practices set out in Section 3 of this Report, will it be possible to show the actual sector-wide nature, frequency, scale and scope of government requests for user data, and generally achieve the goal of enhancing transparency and trust that underpins transparency reporting.

Number and nature of the requests

Objective snapshot

The Companies adopt different approaches, with varying degrees of granularity and diverse terminologies, when reporting on the number and nature of the government requests for user data they receive. Table A in Annex B sets forth the types of numbers that the Companies report, whether they provide information on the subject of the request (i.e. number of accounts, users or identifiers specified in the request), whether they report the country from which the request originated, and whether they disclose the kind of data being sought by the request (e.g. device information, content data).

Since the majority of the surveyed Companies (17 out of 20) are US-based, most of the reporting practices identified in this Report, as well as the government requests to which they relate, follow and are made under US law.

Generally, government requests for user data made under US law can be divided into four main categories: legal process requests,[12] preservation requests, emergency requests and national security requests. Legal process requests are those which the Companies receive from government or law enforcement agencies accompanied by a (domestic) legal process, such as a court order or search warrant. Preservation requests are those on the basis of which governments ask the Companies to preserve existing user data available at the time of the request, typically for 90 days. Emergency requests are those whereby governments ask the Companies to disclose user data without following the required legal process (e.g. without a subpoena or search warrant) where there is an immediate threat of death or serious physical injury. National security requests are orders for user data received under the US Foreign Intelligence Surveillance Act ("FISA") and National Security Letters ("NSLs"). US-based Companies' reporting practices markedly revolve around this classification.

As summarised in Table 1 below, fifteen Companies[13] provide the specific number of government requests they receive for each different type of local (i.e. US-based) legal process. The most common breakdown of local legal process requests is between subpoenas, court orders and search warrants. Conversely, no Company provides a breakdown of international legal process requests (i.e. they are all included in one single group). Moreover, six Companies [14] report the number of preservation requests, and ten Companies[15] disclose the number of emergency requests. All US-based Companies report the number of US National Security requests set out as a range (not a precise figure).[16] On the other hand, two of the three non-US Companies surveyed in this Report break down the number of government requests they receive based on different criteria under their local laws, and none of them provide information on national security requests.

Table 1 - Breakdown of the number of legal process requests and reported categories

Company	*How does the Company report on the number of legal process requests?*	*Reporting on preservation requests?*	*Reporting on emergency requests?*	*Reporting on National Security Requests?*
Amazon	Number of local requests is broken down by different types of US legal processes Number of non-US legal process requests is not broken down by different types of legal processes	No	No	Yes
Apple	Number of local requests (device requests, financial identifier requests, account requests) is broken down by different types of US legal processes Number of non-US legal process requests is not broken down by different types of legal processes	Yes	Yes	Yes
Automattic	Number of local requests is broken down by different types of US legal processes Number of non-US legal process requests is not broken down by different types of legal processes	No	No	Yes
Dropbox	Number of local requests is broken down by different types of US legal processes Number of non-US legal process requests is not broken down by different types of legal processes	No	No	Yes
Facebook	Number of local requests is broken down by different types of US legal processes	Yes	Yes	Yes

	Number of non-US legal process requests is not broken down by different types of legal processes			
Google	Number of local requests is broken down by different types of US legal processes Number of non-US legal process requests is not broken down by different types of legal processes	Yes	Yes	Yes
Kakao	Number of requests is broken down by type of request, including request for communication data, communication-restricting measure, communication confirmation data, and search and seizure warrant	No	No	No
LINE	Number of requests is reported in the aggregate until H1 2017 From H2 2017 the total number of requests is broken down (%) into different categories, including abuse of children, financial harm, bodily harm, illegal and harmful information, unauthorised access, intellectual property infringement and others	No	No	No
LinkedIn	Number of local requests is broken down by different types of US legal processes Number of non-US legal process requests is not broken down by different types of legal processes	No	No	Yes
Medium	Number of requests is reported in the aggregate	No	No	Yes
Meetup	Number of local requests is broken down by different types of US legal processes Number of non-US legal process requests is not broken down by different types of legal processes	No	No	Yes
Microsoft	Number of 'law enforcement' requests is reported	No	Yes	Yes
Pinterest	Number of local requests is broken down by different types of US legal processes Number of non-US legal process requests is not broken down by different types of legal processes	No	No	Yes
Reddit	Number of local requests is broken down by different types of US legal processes Number of non-US legal process requests is not broken down by different types of legal processes	Yes	Yes	Yes
Snapchat	Number of local requests is broken down by different types of US legal processes Number of non-US legal process requests is not broken down by different types of legal processes	No	Yes	Yes
TikTok	Number of 'legal requests' is reported	No	Yes	No
Tumblr	Number of local requests is broken down by different types of US legal processes Number of non-US legal process requests is not broken down by different types of legal processes	No	Yes	Yes
Twitter	Number of local requests (i.e. account information requests) is broken down by different types of US legal processes	Yes	Yes	Yes

	Number of non-US legal process requests is not broken down by different types of legal processes			
Wickr	Number of local requests is broken down by different types of US legal processes Number of non-US legal process requests is not broken down by different types of legal processes	No	No	Yes
The Wikimedia Foundation	Number of local requests is broken down by different types of US legal processes Number of non-US legal process requests is not broken down by different types of legal processes	Yes	Yes	Yes

The Companies use different terms to refer to the same type of request. For example, Reddit uses 'information production requests', Microsoft 'law enforcement requests', TikTok 'legal requests', Facebook 'legal process requests', Snapchat 'criminal legal requests', and Twitter account 'information requests' to refer to government demands to access user data other than emergency requests and US National Security Requests.[17]

Two Companies[18] combine local and international requests in one group, reporting aggregate numbers. Fourteen Companies[19] break down the requests they receive by country, whereas four Companies[20] only distinguish between local and international requests.

Seventeen Companies[21] report numbers of the subject of the request (i.e. numbers of the accounts, users, URLs or other identifiers specified in the request), although they use different terminology to refer to those subjects.[22] Conversely, only two Companies[23] provide explicit information on the type of data sought by the request, whilst six Companies[24] provide this information indirectly.[25]

Trends and insights

Overall, the Companies' transparency reports mainly focus on 'targeted' law enforcement requests. Conversely, largely due to disclosure restrictions mandated by law, they tend to provide very limited information, if any, about national security and foreign intelligence requests. Therefore, whilst valuable information concerning the former type of requests can be derived from the Companies' transparency reports – thereby enabling some scope for comparison and assessment – these reports do very little to overcome the general lack of transparency about bulk data collection or unlimited government access to data made under the latter type.

Law enforcement (or legal process) requests

The Companies' current reporting practices allow us to determine the number of global (i.e. domestic plus international) government requests for user data that each Company receives during the relevant reporting period.[26] These numbers can be found in Section 1 of the Companies' profiles in Annex C. Given that fourteen Companies break down the requests they receive by country, it is also possible to some extent to identify from which countries the greater number of requests originate. When numbers of requests broken down by country are consistently reported over the years, it is possible to identify trends in the reported data, such as period-on-period fluctuations in the number of requests from a specific country.[27]

Moreover, most US-based Companies tend to provide a good level of granularity regarding the local 'legal process' requests they receive, breaking down the number of said requests into different categories of US legal processes (typically subpoenas, search warrants, court orders and other orders). This breakdown has great informative value, since different legal processes are required to access different types of data.[28] For example, as search warrants are required for the disclosure of content data,[29] a higher number of

search warrant-based requests compared to previous reporting periods may suggest greater demands for content information by US government and law enforcement agencies.

However, such degree of granularity applies to local requests only, as the Companies group together all international (i.e. non-US) legal process requests they receive in one single category. This less detailed treatment of international legal process requests is understandable on account of two considerations. Firstly, the applicable laws of the different (oftentimes multiple) jurisdictions in which the Companies operate likely contemplate dissimilar types of legal process requests which cannot be equated with those of other countries.[30] And secondly, following US law, international requests for content and non-content data are typically conducted through a Mutual Legal Assistance Treaty (MLAT) process; however, it is not always possible to know whether a court order originated through domestic (i.e. US) process or through the MLAT process, or from what country it originated when it is issued through the MLAT process.[31]

Nevertheless, a number of US-based Companies also operate from other regions,[32] yet they do not break down the requests they receive from the government of their alternative place of establishment based on the different types of legal processes contemplated in said regions' local laws. This raises the question of whether transparency reporting can help elucidate current practices, including in non-OECD members and particularly those that may cause distrust in the digital economy and thus hamper the flow of data.

Also, few Companies report numbers of preservation requests and emergency requests. This raises the question of whether the Companies which do not specifically report on these requests include them in their legal process category, or whether they exclude them altogether from their reports. Further, as noted previously, some Companies use different nomenclatures to refer to the same type of (legal process) request. The use of different terms to refer to the same issue, as well as dissimilar reporting of preservation and emergency requests, reveal two aspects of transparency reporting that would benefit from standardisation. The use of different terms to refer to the same topic is likely to bring about confusion. In turn, when only few companies report data on preservation and emergency requests, the informative value of that data is limited, since no sector-wide comparisons or assessments can be made.

Subject of the law enforcement requests

The Companies use a variety of terms to describe the subjects of the requests they receive – i.e. an account, user, website, URL or another identifier – highlighting another area of transparency reporting in need of standardisation.[33] Reporting on the subject of the request is essential to determine the universe of users that can be potentially impacted by the requests (i.e. users whose data will be disclosed if the request is accepted); the total number of requests, in and of itself, reveals nothing about government requests' actual scale and scope. However, since the Companies are reporting on somewhat different yet related data points associated with the subjects of requests, the data the Companies report in this connection cannot be compared. Consequently, no industry- or sector-wide trends and developments concerning the actual scale and scope of government requests can be detected, such as increases or reductions in the number of individual records or accounts specified in them.

The reporting on the number of requests in which specific data was sought (e.g. 'content data', such as posts or comments, or 'non-content data', such as subscriber name or email address) can provide additional, valuable information, shedding light on government requests' targets and the extent to which they may impinge upon individuals' privacy. Regrettably, only two Companies disclose specific numbers on the data being sought by government requests. To enhance the informative value of the Companies' transparency reports and enable meaningful analysis and comparison amongst them, the reporting of this metric, which is currently rather exceptional, must become widespread.

National security requests

The ability of transparency reports to reveal the scale, scope and impact of government access requests is significantly impaired when local laws place restrictions on the companies' reporting of certain requests. A case in point are the restrictions imposed by US law on US-based companies' ability to report on national security requests, which are typically accompanied with non-disclosure or 'gag' orders. Prior to January 2014, US-based companies were not able to even acknowledge having received national security requests. After a settlement between Facebook, Google, LinkedIn, Microsoft and Yahoo with the US Department of Justice,[34] these companies were allowed to report on these requests under two possible reporting structures. One structure authorised the reporting on numbers of national security letters (NSLs), Foreign Intelligence Surveillance Act (FISA) orders for content, and FISA orders for non-content in bands of 1 000, whilst under the other structure companies could report numbers in bands of 500 provided that all requests were reported in the aggregate. The passing of the 2015 USA FREEDOM Act relaxed the aforesaid restrictions significantly, making available four alternative reporting structures;[35] however, actual numbers must be still reported in bands (of 1000, 500, 250 or 100, depending on the chosen reporting structure).

While reporting in bands may work to some extent for companies that typically receive a high number of national security requests, the currently-allowed bands remain too wide for small Internet-based companies. For example, if a company like Wickr receives five such requests per reporting period, users will not have an accurate sense of the actual volume of national security requests Wickr received, as Wickr will have to report either 0-99, 0-249, 0-499 or 0-999, depending on the chosen reporting structure. If Wicker chose the reporting structure in bands of 100, the high end of this permitted range (99) would be equal to the number of all US non-national security requests Wickr received during H1 2019.[36] Reporting in this way obfuscates rather than illuminates the volume of national security requests a small company receives, and likely leads to speculation about the level of interest in a service by the US government, suspicion and lack of trust from users and the public at large. Crucially, reporting in this fashion is insufficient to dissipate the concerns of governments having potentially unfettered access to privately-held data in the context of national security and foreign intelligence investigations. The difficulty here, however, is that more granular reporting can allow an adversary to determine a state's capacity or workload regarding collection efforts. Any public facing report needs to balance these competing interests.

Outcome of the requests

Objective snapshot

The Companies' approach to reporting the outcome of the requests is also far from uniform, as there are different degrees of specificity and dissimilar reporting metrics. Table B in Annex B lists the Companies' reported response to the requests (i.e. the action the Company performed after analysing the request), the breakdown of the response (e.g. number of cases where the request was fully or partially complied with) and the reporting on the number of accounts and/or users impacted by the request (i.e. the number of specified accounts or users in respect of which data was disclosed in response to the request).

The majority (thirteen) of the Companies[37] reports the production or disclosure of information as their unique response to government requests, whereas four Companies[38] also report challenging, rejecting or partially complying with the requests as an alternative response. Kakao stands out for being the only Company reporting the 'processing' of the request as its single response, without specifying exactly what processing a response means. Wickr, on the other hand, does not report what their response was.

The most striking divergence of approaches lies in the Companies' breakdown of their response to the requests. As seen in Table 2 below, ten Companies[39] provide no breakdown, only reporting the number or percentage of total requests where information was produced in reply to the request. At the other end of the spectrum, two Companies[40] provide a detailed breakdown of their responses, indicating the number of requests where data was provided, number of requests challenged in part or rejected in full, number of requests where non-content data was provided and number of requests where content data was provided. Between the two extremes, different degrees of granularity can be seen, with Dropbox and Microsoft providing a somewhat detailed level of specificity in their responses' classification, and Facebook, Amazon and Tumblr reporting rather less granular – albeit still useful – classes of metrics. LINE reports a curious breakdown into percentage of handled requests and number of cases where data was provided, without explaining the actual distinction between the two scenarios.

Table 2 - Breakdown of the reply to the request

Company	*Breakdown of the reply to the request*
Amazon	Number of requests with full response, partial response, no response.
Apple	Number and % of device requests where data was provided. Number and % of financial identifier requests where data was provided. Number of account requests where no data was provided, number of account requests challenged in part or rejected in full, number of account requests where only non-content data was provided, number of account requests where content data was provided and % of account requests where data was provided. For preservation requests, number of accounts where data was preserved. For emergency requests, number of requests rejected/challenged & no data provided, number of requests where no data was provided, and number and % of requests where data was provided.
Automattic	No breakdown. Only the % of requests where some or all information was produced is reported.
Dropbox	Number of requests where data does not exist, no information provided, non-content data provided and content data provided (for US requests only).
Facebook	% of total requests where some data was produced, % of emergency requests where some data was produced, and % of legal process requests where some data was produced.
Google	No breakdown. Only the % of requests where some data was produced is reported.
Kakao	No breakdown. Only the number of processed requests is reported.
LINE	% of handled requests and number of requests where data was provided.
LinkedIn	No breakdown. Only the % of requests for which LinkedIn provided some data is reported.
Medium	No breakdown (as Medium received zero requests).
Meetup	Number of rejected requests, requests where content was disclosed and requests where only non-content was disclosed.
Microsoft	Number and % of content disclosures, number and % of non-content disclosures, number and % of requests where no data was found and number and % of rejected requests.
Pinterest	No breakdown. Only the number of total requests where information was produced is reported.
Reddit	No breakdown. Only the number of information production and emergency requests where account information was disclosed is reported. For preservation requests, Reddit discloses the number of requests complied with.

Snapchat	No breakdown. Only the % of legal requests and emergency requests where some data was produced is reported.
TikTok	No breakdown. Only the % of requests where some data was produced is reported.
Tumblr	% of blog content produced, % of account data produced and % of compliance.
Twitter	For account information requests, % of requests where some information was produced, % of narrowed requests, and % of cases where content information and cases where non-content information was provided. For emergency requests, % of requests where some information was produced.
Wickr	No breakdown.
The Wikimedia Foundation	No breakdown. Only the number of total requests where information was produced is reported.

The number of accounts or users impacted by the request (i.e. the number of specified accounts or users in respect of which data was disclosed in response to the request) is an important yet not widely reported figure. It must be distinguished from the subject of the request metric referred to in the preceding section (i.e. number of accounts, users or identifiers specified in the request), as the fact that an account or user is specified in a request does not entail that the same is ultimately affected - that data about that account or user may not be ultimately disclosed in response to the request. Only five Companies[41] have reported on the number of accounts or users impacted, with Apple and Reddit ceasing this practice in their last transparency reports.

Trends and insights

The reporting on the outcome of the request is the area where greater disparities are found. As a consequence, much of the reported data cannot be readily compared across the Companies.

Currently, the only metric concerning the outcome of the request that can be compared across the Companies is the number or percentage of requests where information was produced (given that sixteen Companies report it). This metric, in and of itself, is hardly instructional. Important questions follow from this single reported outcome, such as whether all requested information or only part of it was produced, what information was produced, and why no information was produced in the remaining cases (i.e. was the request challenged, rejected or no information was found?). A select group of Companies (Twitter, Apple, Dropbox and Microsoft) engage in more granular reporting on the outcome of requests, such that it is possible to answer these questions. Nevertheless, the fact that detailed reporting of this type is exceptional means that important sector-wide trends cannot be detected, such as increases or reductions in the number of requests challenged by the Companies, or fluctuations in the numbers of cases where content and/or non-content data was disclosed.

Moreover, the outcome of the requests cannot be fully depicted if the number or percentage of accounts and/or users impacted by them is not reported. Only on the basis of this information is it possible to appreciate the actual magnitude of governments' access to user data held by private entities. Since the majority of the Companies disclose numbers of government requests on a per country basis, uniform reporting of accounts and/or users impacted on this basis would allow the reader to identify which government access requests are most successful. Yet, as seen above, the reporting on the number of accounts/users impacted by the requests is not widespread. As a result, the sector-wide available data that can be used to analyse and understand the Companies' responses to government requests is of very limited informative value, only allowing the reader to determine the universe of cases where user information was fully or partially disclosed, yet not the actual number or volume of such information.

Importantly, by reporting on both the subject of requests (i.e. user, accounts or other identifiers) specified in government requests **and** the number of subjects actually impacted by them, the Companies can provide valuable information to enable an analysis of the rate with which data is produced in response to government access requests. Currently, however, only the Wikimedia Foundation reports on these two metrics, so no sector-wide developments can be identified. Notably, Apple and Reddit have ceased to report the number of users/accounts impacted. This decision has diminished the instructional value of their transparency reports', and may signal a counter-productive trend towards more opacity in the reporting of the Companies' actions in response to government requests for user data.

Indication of the legal processes required to access different types of information / Explanation of international requests processing

Objective snapshot

Empirical research published in 2014 indicates that laws that authorise governments' access to privately-held data have different standards for access to different kinds of information (e.g. real-time interception of communications versus access to stored communications) contemplate a variety of limits and control on government access, and generally tend to be vague and ambiguous (Rubinstein, Nojeim and Lee, 2014, p. 97). Crucially, that research found that government interpretations of these laws are often hidden and even classified (Rubinstein, Nojeim and Lee, 2014, p. 97). Accordingly, it is of the essence that the reporting Companies indicate which types of legal processes are required for them to produce and disclose specific kinds of user data, and how they interpret these applicable laws.

Moreover, in the light of the general rules on territorial jurisdiction, no firm is bound to abide by orders passed by foreign agencies unless a local court or authority instructs them to do so. To be sure, companies can respond to international requests on a voluntary basis, in accordance with their own policies. However, if no voluntary disclosure of information in response to international requests is contemplated in the policies of the addressee of an international request, this request must be subject to appropriate legal mechanisms to be binding in the jurisdiction where the addressee of the request is based. Therefore, it is crucial that the reporting Companies explain with sufficient clarity under which circumstances they voluntarily comply with a foreign request, and what channels international agencies must follow to endow their requests with a binding force.

Section 2 of the Companies' profiles in Annex C sets out the Companies' explanations on these two matters.

With the notable exception of Meetup, all of the Companies have explicit policies on disclosure of user information in response to local requests, detailing specifically which type of legal process must be followed for the disclosure of particular kinds of data. In particular, seventeen Companies[42] explain that a subpoena is required to disclose non-content data, whilst search warrants or court orders are a precondition to turn over content information. Some Companies go the extra mile and explain the information government and law enforcement agencies may access through other less common (US) legal processes, such as wiretap orders and pen register orders.[43]

No Company contemplates the voluntary disclosure of information in response to international law enforcement requests. However, this common no voluntary disclosure rule typically does not apply in cases of emergency (i.e. emergency requests), provided that the relevant Company is satisfied that there is an actual threat to individuals' physical integrity and lives.

Similarly, with the exception of Kakao and Meetup, all of the Companies provide an explanation of the process international agencies and governments must follow to endow their requests with a binding force,

although with varying levels of detail. Whereas five Companies[44] offer somewhat brief explanations, three Companies,[45] conversely, stand out for their detailed descriptions. The remaining Companies' approaches to supplying information on international requests processing lie between the two extremes.

Trends and insights

It is a positive trend that most Companies explain which type of legal processes are required in order for them to disclose specific kinds of user data, and how they interpret the applicable laws detailing such legal processes. This information helps dissipate concerns about the perceived lack of transparency with regard to the legal mechanisms governments rely on to access privately-held data, thereby increasing certainty and fostering trust. The absence of voluntary disclosure of information to foreign governments reinforces certainty and trust, as users of the Companies' services can be assured that disclosure is only possible on the basis of clearly-defined legal processes and in international emergencies.

Save for a few exceptions,[46] the Companies tend to be brief in their explanations as to the processes that international governments must follow to obtain a response to their access requests. These explanations typically note that international entities must follow a Mutual Legal Assistance Treaty (MLAT) process or letter rogatory process. The Companies' transparency reports would likely improve significantly if they explained how requests processed through an MLAT process or letter rogatory are counted and reported.

Indeed, the opacity surrounding the computation methodology of these requests has important ramifications. For example, Facebook states that requests received through the MLAT process are included in Facebook's reports, but Facebook is unable to identify the precise number of requests it receives through this channel since they result in the issuance of a search warrant or court order under US law which do not always indicate that they are the product of an MLAT request. A natural question that follows is how are MLAT requests counted, i.e. are they reported as domestic requests or international requests? In this vein, Dropbox notes that in H1 2019 it received five requests pursuant to MLATs in place between the United States and foreign countries (requests from Germany, Sweden, Canada, the Netherlands and Australia), and that it included these requests in its reporting on domestic (i.e. US) requests.[47] This approach is problematic, since the number and magnitude of US requests can be overstated, and foreign requests concomitantly downplayed.

Apple adopts what appears to be the most sensible practice in this regard. In its last report, Apple identified 11 MLAT requests for information that were issued by the US government in H1 2019. However, Apple notes that this might have not been the precise number of MLAT requests received, as in some instances a US court order or search warrant may not indicate that it is the result of an MLAT request. In instances where the originating country was identified, Apple counted and reported the MLAT request under the country of origin. In instances where the originating country was not identified, Apple counted and reported the request under the US. The diversity of approaches concerning the reporting of MLAT requests singles out yet another aspect of transparency reporting in need of standardisation to enhance the reliability and clarity of the reported information.

Reporting on user notifications

Objective snapshot

Transparency is an important means of ensuring trust in an organisation, particularly where it handles personal data. In order to foster trust amongst its users, companies can notify impacted users before surrendering their data to government and law enforcement agencies (subject to clearly articulated limitations such as when prohibited from doing so by law or in emergencies). Trust and transparency can

be enhanced even further through the reporting of specific figures about cases where the users specified in the requests were notified prior to the production and surrendering of information. Table 3 below sets forth which Companies have published a clear policy on user notifications, and which Companies report figures regarding notifications provided to users before they disclose user information. Please see Sections 3 and 1 of the Companies' profiles in Annex C for detailed explanations of the relevant policies and reported numbers.

Table 3 – Policy and reporting on user notifications

Company	*Publicly available information on the Company's policy on user notifications*	*Reporting of figures regarding notices provided to users*
Amazon	Yes.	No.
Apple	Yes.	No.
Automattic	Yes.	No. However, Automattic reports the % of US requests accompanied with a non-disclosure order.
Dropbox	Yes.	Yes. Dropbox reports the number of requests and accounts specified where notice to users was provided, broken down by US legal process type, that is, search warrants, subpoenas and court orders.
Facebook	Yes.	No.
Google	Yes.	No.
Kakao	No.	No.
LINE	Yes.	No.
LinkedIn	Yes.	No.
Medium	Yes.	No.
Meetup	No.	Yes. Meetup reported the number of requests with non-disclosure orders, the number of cases where there was no non-disclosure order and notice was provided, and the number of cases where there was no non-disclosure order and notice was not provided.
Microsoft	Yes.	No.
Pinterest	Yes.	Yes. For US government requests, Pinterest reports the number of accounts notified. Accounts notified means that the account owner was notified before the disclosure of information.
Reddit	Yes.	Not anymore. In the 2014 TR, Reddit reported the No. of requests with legally binding gag orders. That data is absent in subsequent transparency reports.
Snapchat	Yes.	No.
TikTok	Yes.	No.
Tumblr	Yes.	Yes. Tumblr discloses the % of cases with non-disclosure order. Also, Tumblr brakes down the cases where it complied at least in part with requests for user information into different categories of investigations, including bullying/harassment, invasion of privacy, national security and cybercrime, suicide, violent crimes, other investigations, and harm to minors. Percentages of cases where notice to users was given and not given are disclosed in each category.
Twitter	Yes.	Yes. Twitter reports the percentages of account information requests under seal

		(i.e. where there is a court order prohibiting Twitter from notifying affected users or anyone else about the request prior to disclosure, or local law prohibits Twitter from providing notice), requests where user notice was provided (i.e. the requests in which Twitter attempted to notify the affected users prior to disclosure), and requests not under seal and no notice provided (cases where no data was disclosed in response to the request, for example, the request was withdrawn prior to disclosure or the request was defective).
Wickr	Yes.	Yes. Wickr reports the number of accounts receiving notice of the request.
Wikimedia Foundation	Yes.	Yes. The Wikimedia Foundation reports the number of user accounts notified.

Save for Kakao and Meetup, all of the Companies have published a clear stance on user notification in case of government requests for user data, detailing the circumstances under which such notification does not take place.

Conversely, the practice of reporting numbers or percentages of user notifications is significantly less widespread. Only seven Companies[48] engage in this practice. It must be noted that Tumblr no longer does so since H1 2017 (after its numbers began to be published in combination with Oath's brands). Also, Reddit used to provide the numbers of requests subject to non-disclosure orders (in which case no notification is given), but stopped this practice as from its 2015 transparency report.

Trends and insights

The publication of a policy on user notification in cases of government requests for their data is one of the few aspects of transparency reporting where constructive uniformity can be seen. Under the Companies' current reporting practices, users have the reassurance that their data will not be disclosed without prior notice unless in narrowly defined emergency situations, when doing so would be counter-productive or ineffective, or otherwise as prohibited by law (such as when the request is subject to a non-disclosure order).

Although such reassurance is positive, however, current practices make it difficult to determine the extent to which Companies' policies and legal requirements prohibit them from notifying users prior to disclosing their personal data in accordance with a government access request. Specifically, Companies tend not to report statistics regarding how often they provide notice to users prior to disclosure. Reporting these statistics would likely reinforce the Companies' commitment to protect their users' fundamental rights and freedoms, particularly their rights to privacy and data protection. Reporting these statistics would also likely foster more trust regarding the Companies' data handling practices.

Reporting on the products and services targeted by the requests

Objective snapshot

Some Companies offer multiple products and services, sometimes as offshoots from the main product or service that they offer. For example, Google's main product is the search engine Google Search, but it also offers a plethora of other products and services such as Google Maps, Gmail, Blogger, Chrome and YouTube. Another example is Facebook, which in addition to its core product - the Facebook social network - provides other popular services such as Instagram, WhatsApp and Facebook Messenger. As will be seen below, Companies offering more than one product or service adopt different approaches to the reporting on which service is the subject of a government access request. Table 4 below provides an overview of these approaches, excluding single-product Companies.

Table 4 – Reporting on the services targeted by the requests

Company	*Reporting on the services targeted by the requests*
Amazon	Amazon reports 'all requests received by Amazon' in one single group until H2 2017. From H1 2018 onwards, Amazon reports total requests and Amazon Web Services requests separately. Amazon does not specify which specific products and services are included in 'total requests'.
Apple	Apple does not specify which product or service is the subject of government requests.
Automattic	Automattic does not specify which product or service is the subject of government requests.
Facebook	Facebook states that its reports include information about requests related to its various products and services including Facebook, Instagram, Messenger, Oculus and WhatsApp, unless otherwise noted. Facebook reports all the government requests it receives in the aggregate, without providing specific numbers for each product or service.
Google	Google reports cases where a government agency asks Google to disclose information about someone who uses 'Google services'. Google does not specify which specific services are included in that term, but does indicate that government agencies commonly request information from Gmail, YouTube, Google Voice and Blogger. Google reports all the government requests it receives in the aggregate, without providing concrete numbers for specific products or services.
Kakao	Kakao reports the government requests it receives broken down into requests received by Daum and requests received by Kakao.
LINE	LINE notes that the reports prior to and including H1 2018 include data related to the LINE messaging app only. The reports for Jul-Dec 2018 and onward cover data related to all services that LINE Corporation provides. Any data from services provided by LINE subsidiaries and affiliates is not included in its reports. LINE reports all the government requests it receives in the aggregate, without providing specific numbers for each product or service.
Microsoft	Microsoft does not specify which product or service is the subject of government requests.
Tumblr	After its acquisition by Verizon Media in 2017, Tumblr's numbers are combined with Oath's other brands, including AOL and Yahoo.
Twitter	Twitter reports specific figures for its services Vine and Periscope as from H1 2016, including the total number of information requests each received, and the percentage of cases where information was disclosed. Twitter clarifies that the Requests for Vine and Periscope account information are included in the Twitter's total number of government requests. As from H1 2017, Twitter also reports the number of Vine and Periscope accounts specified in the requests.
Wikimedia Foundation	The Wikimedia Foundation does not specify which product or service (i.e. Wikimedia project) is the subject of government requests.

Of the ten Companies that operate more than one product or service, four[49] provide no information on which products and services are included in their transparency reports, let alone specific numbers on a per product basis. Google gives examples of products which are most commonly targeted by government agencies, without further breakdown. LINE clarifies with more precision which of its services are included in its reports, but discloses total numbers in the aggregate. Facebook provides more clarity as to which of its products are included in its transparency reports, but also discloses total numbers in the aggregate. Amazon's reporting approach makes it clear that its reports include data from Amazon Web Services, the numbers of which are reported separately, and data from all of other Amazon's products, without specifying which of those in particular. Only Twitter and Kakao indicate with precision which services are included in their reports, disclosing concrete figures on a per service basis.

Trends and insights

The most common approach amongst multi-product Companies is the reporting of all requests they receive in the aggregate, without providing separate figures on a per service basis. This is likely the preferred approach due to the challenges multi-product Companies face when trying to separate different services that are highly integrated with one another and are typically accessed through one single account, as is the case of Facebook/Facebook Messenger, Google's Gmail/YouTube/Google Search and Microsoft's Outlook/Office/Skype. However, this argument is weaker in relation to stand-alone products and services (e.g. Instagram, Wordpress.com).

When specific numbers about government requests for user data are disclosed per individual product, a transparency report can depict more accurately how said requests are impacting the reporting firm's array of offerings, highlighting differences in impact between its services. Moreover, if granular reporting of this type were a widespread practice, it would be possible to compare such impact with that experienced by other companies' comparable services. Regrettably, reporting of this kind is rather exceptional, thus highlighting an area of transparency reporting where more specificity would result in more potentially meaningful data.

Frequency with which transparency reports are issued

Objective snapshot

There is no industry-wide standard for the frequency with which companies should publish transparency reports. As a consequence, the publication timeframes for transparency reports range from quarterly to annual publication schedules. Table 5 below sets forth the period covered by each Company's first transparency report, the frequency with which their transparency reports are issued, and the period covered by their last transparency report.

Table 5 – Reporting periods

Company	*Period covered by first transparency report*	*Frequency with which transparency reports are issued*	*Period covered by last transparency report*
Amazon	H1 2015	Every six months	H2 2019
Apple	H1 2014	Every six months	H1 2019
Automattic	H2 2013	Every six months	H1 2019
Dropbox	2012	Every six months since 2014	H1 2019
Facebook	H1 2013	Every six months	H1 2019
Google	H1 2011	Every six months	H1 2019
Kakao	H1 2012	Every six months	H1 2019
LINE	H2 2016	Every six months	H1 2019
LinkedIn	H2 2012	Every six months	H1 2019
Medium	2014	Only one transparency report has been issued	2014

Meetup	2016	Only one transparency report has been issued	2016
Microsoft	H1 2013	Every six months	H1 2019
Pinterest	Q3 2013	Every three months	Q4 2019
Reddit	2014	Every year	2019
Snapchat	Period between 1 November 2014 and 28 February 2015.	Every six months since 2015	H1 2019
TikTok	H1 2019	Every six months	H1 2019
Tumblr	2013	Every six months from H1 2014 to H2 2016.	H2 2016
Twitter	H1 2012	Every six months	H1 2019
Wickr	Period between 26 June 2012 – 25 February 2013	At random intervals, on a quarterly basis, and on a half-yearly basis since H2 2018	H2 2019
Wikimedia Foundation	July 2012 – June 2014	Every six months since H2 2014	H1 2019

The majority of the Companies have been consistent in publishing their transparency reports. Whilst Dropbox, Snapchat, Tumblr and the Wikimedia Foundation changed their reporting periods after issuing their first transparency report, they have been regular in their publishing schedule after that change. Wickr is the exception, having published many transparency reports at random intervals, then on a quarterly basis, and recently on a semi-annual basis.[50] Moreover, some Companies – Medium and Meetup - have stopped issuing transparency reports after their first release, whereas TikTok has recently issued its first report covering H1 2019. Since its acquisition by Verizon Media in 2017, Tumblr stopped publishing transparency reports at company level; its numbers were combined with the numbers of all other Verizon Media's brands as from that year.

Trends and insights

The most basic and fundamental best practice in transparency reporting is the regular issuance of reports on a consistent timeline. Although publication on a biannual timeframe is the most common approach to reporting, the absence of a standard publication schedule means that transparency reports cannot be easily compared, which impinges upon their informative value.

The fact that there are more Companies that stopped issuing transparency reports than Companies adopting this practice for the first time suggests that transparency reporting may be losing momentum. Figure 1 in Section 1 seems to confirm this trend.

The case of Tumblr highlights potential transparency setbacks that may arise when a company faces a change of administration (whether as a result of an acquisition, merger or otherwise). Having published regular, company-level transparency reports up until H2 2016, after its acquisition by Verizon Media in 2017, Tumblr's government requests are reported in the aggregate with the requests received by all of Oath's (one of Verizon Media's subsidiaries) brands, including AOL and Yahoo.[51] Therefore, it is not possible to ascertain with precision anymore the magnitude of the government requests for user data that Tumblr receives, or the manner in which Tumblr responds to said requests. This does not have to be the

case: after LinkedIn was acquired by Microsoft in 2016, LinkedIn has continued to publish transparency reports individually, without merging its numbers with Microsoft's other services.

3. Good practices in transparency reporting

As seen in preceding Section 2, the Companies' reporting approaches tend to differ significantly. Consequently, save for a few broad metrics that are uniformly reported, most of the reported information cannot be easily compared. This is an undesirable outcome, since in the absence of easy comparability amongst the reports, it is highly difficult, if not impossible, to derive clear information as to the actual scope of governments' data access requests and the extent to which access is granting accordingly.

Ambiguity as to the extent to which governments are granted bulk or potentially unlimited access to privately-held information runs counter the goal of reinforcing trust in the digital economy and facilitating trust-based transborder data flows.

Against this backdrop, this Section sets forth a number of good practices in transparency reporting, the implementation of which can enhance transparency, provide more clarity, achieve more standardisation and enable greater comparability amongst reports.

Number and nature of the requests

When it comes to transparency reporting, as a general rule of thumb, the more granularity, the better. It is important, however, to keep in mind that for many companies, the biggest barrier for engaging with transparency reporting is operational. Reporting schemes are onerous, and voluntary ones may not be viewed by companies as ultimately being worth it. A balance must therefore be found between a standardised comprehensive reporting system and one that is not too costly.

At a minimum, all reporting companies should report separately on the number of requests they receive over a clearly delineated time period, for each different type of legal process and/or category of request. On this basis, policy-makers, researchers, analysts and the public can identify which types of requests are more common. This information can provide highly valuable insights. For example, a higher number of a specific type of legal process request may suggest that its evidentiary requirements are too lenient, and therefore legal reform should be contemplated. Also, where a particular request is required to surrender private information (e.g. a search warrant to disclose content data), a higher number of those requests may be indicative of a higher impact on individuals' privacy.

Numbers and percentages should also be reported on a per country basis. Reporting in this fashion allow readers to determine which countries are the main or most aggressive requestors of user data, provided companies in those jurisdictions are allowed to report such statistics. A company that reports consistent metrics over consistent time periods also allows the reader to detect changes and trends in the frequency with which specific countries request access to user data.

Crucially, by reporting on the numbers of users, accounts, URLs or other identifiers that are the subject of each government access request, researchers can identify the intended reach and potential impact of such requests. Accordingly, all reporting entities should report this metric. Companies should clearly explain how they define the "subject" of data access requests, to avoid any confusion or ambiguity.

Moreover, the terms 'user data' or 'user information' are overly broad, encompassing a wide range of information, some of which individuals may deem highly sensitive and consequently could cause great distress if covertly accessed by government agencies. At the same time, individuals may consider some information inconsequential. Therefore, reporting companies should ideally provide figures on the type of data which is sought by the requests they receive. It is true that this type of information can be inferred from the type of legal process law enforcement and government agencies rely upon to access user data; however, it is unlikely that people lacking knowledge of such processes and their intricacies can make such an inference. Whilst reporting on the number of requests where content data was provided and non-content data was provided is a step in the right direction, reporting companies should ideally do more.

Outcome of the request

Section 2 of this Report demonstrated that the Companies have adopted a variety of approaches to reporting on how they respond to government requests for user data. Reporting this information is likely to be challenging, as the Companies' responses to certain requests may be hard to quantify, such as when a request is challenged but nevertheless results in a full or partial disclosure of information.[52]

Nevertheless, on account of the multiple scenarios that can be derived when requests are challenged, rejected and/or partially complied with, clear and granular reporting on the requests' outcomes is particularly important. Ideally, companies should report their responses for each different type of process or request category (e.g. warrant, subpoena, emergency request), breaking them down into the different actions they performed (e.g. challenged requested, rejected request, some information provided, all information provided).

Furthermore, the outcome of requests cannot be fully appreciated if the number or percentage of accounts and/or users impacted by them is not reported. Only on the basis of this information it is possible to appreciate the scale and magnitude of government and law enforcement agencies' success when demanding user data. Additionally, if companies report on both the subject of the requests specified in government demands and the number of subjects impacted by them, governments' user data requests success rate may be determined with greater or lesser accuracy. Accordingly, to the extent possible, all companies engaged in transparency reporting should provide these two metrics.

Indication of the legal processes required to access different types of information / Explanation of international requests processing

Informative and comprehensive reporting on the specific types of legal processes government and law enforcement agencies must follow to access privately-held data is essential to remove concerns about potential overly-permissive interpretations of applicable laws granting governments undue or excessive access. At a minimum, reporting companies should explain what are the applicable laws governing government requests for user data, what processes are contemplated thereunder, and what type of information they may disclose in response to each type of process.[53]

Also, in addition to explaining the procedures that foreign government and law enforcement agencies must follow to access the reporting entities' private data (e.g., a Mutual Legal Assistance Treaty (MLAT) process or letter rogatory process), transparency reports should always include an explanation on how international requests that follow such procedures are computed and reported. In the absence of this explanation, readers of transparency reports are likely to find it difficult to determine whether these international requests are counted as local or international requests.[54] As a result, the clarity and informative value of transparency reports is bound to suffer.

Reporting on user notifications

Given the tension between different and competing rights and interests (e.g. public safety, national security, law enforcement and privacy), reporting companies must have a clear policy on the circumstances under which they do and do not provide notification to users when governments require access to their data. Notifications give users an opportunity to defend themselves against and challenge unwarranted, unfounded and/or overarching government requests for their data.

Overall, most Companies show the good practice of having defined and published a clear stance in this regard.[55] This should be the standard in transparency reporting.

A step further to enhance transparency is the reporting of specific figures on user notifications in the context of government requests for user data.[56] Widespread reporting on user notifications would allow for more meaningful analyses and comparison. For example, dramatic changes across the Companies' numbers of requests where user notification was not provided may suggest that a government is increasingly relying on non-disclosure orders, a concerning practice that undermines individuals' privacy.

At a minimum, reporting companies should report the number or percentage of government requests where notification was provided and not provided. To increase transparency even further, reporting companies can provide information on why user notification was not provided in a given case (e.g. there is a court order or local law prohibiting the notification).

Reporting on the products and services targeted by the requests

Multi-product Companies can enhance the clarity of their transparency reports by indicating with precision which of their products are included in them. This holds particularly true for Companies that operate multi-sided platforms having a 'free' and a 'paid' side (e.g. social networks offering users access to the platform at no cost, but charging fees to advertisers that target ads to social network users), as it is not clear whether only the free or both sides are included in the reports.

Also, the provision of figures on a per product basis can expand the scope for comparison amongst reporting companies' comparable services.

Therefore, reporting companies should engage in clear and granular reporting in this area, reporting specific numbers per each product or service included in their reports (e.g. number of requests, percentage of requests where information was produced and number of accounts specified in the request).

Frequency with which transparency reports are issued

The most basic and fundamental best practice in transparency reporting is the regular issuance of reports on a consistent timeline.

However, Section 2 showed that the Companies adhere to different publication schedules, although publication on semi-annual basis is the most common approach. Ideally, transparency reports should adopt the same reporting time periods so that they can be readily and seamlessly compared.

Moreover, companies should consistently publish transparency reports, even if the report simply says that the company received no access requests from governments during the relevant reporting period. This should be a regular practice, integrated into the company's policy regarding transparency reporting. Medium, for example, has published only one transparency report, where it disclosed that it received no

request of any kind during the reporting period. Unfortunately, it has not released any further reports and has not explained the reason for this.

Notable reporting practices

Some Companies adopt notable reporting practices that are worth highlighting.

In the last pages of its transparency reports, Apple includes the section 'Matters of note in this report', where it presents specific facts about certain countries and their requests (e.g. Australia – high number of devices specified in the requests predominantly due to a theft investigation) and the number of MLAT processes identified during the reporting period.

In the section 'Beyond the numbers' of its transparency reports, Dropbox provides interesting trends and statistics (e.g. compared to the last reporting cycle, Dropbox received 15% more warrants, 13% fewer subpoenas and 4.3% more court orders). Reddit and LINE provide similar information throughout their reports.

Generally, Twitter's transparency reporting is very comprehensive. It displays a month-by-month trend graph for government data requests on a per country basis, and also provides a map that shows global trends in government data at a glance, along with a narrative analysis of changes and trends in the data. Facebook's transparency reporting efforts are also noteworthy. In addition to reporting the year-on-year growth of government requests for user data, Facebook provides a ranking of the countries submitting the highest numbers of requests.

Several platforms allow users to download their report data in CSV (comma separated value) format. This format is most helpful to researchers, journalists and others who want to analyse the data, as it simplifies the data extraction process and makes reports – as well as the underlying data behind the information they present - more accessible by design.

The Wikimedia Foundation reports the name of the government agencies issuing the requests. For example, in its last report, the Wikimedia Foundation reported that the federal police of Brazil, the cyber police of India, and the state policy of Italy made informal requests (i.e. not following adequate legal processes to access the user data), and that a local court of France sent a formal request.

Admittedly, the notable reporting practices highlighted above may not be feasible for all companies out there, as engaging in them likely entail costs not every business can incur. Nevertheless, they should become standard practice to the extent possible, as they offer a chance to add additional transparency and information.

4. Recommendations for next steps

The need for consistency in transparency reporting practices

This Report has stressed that the surveyed Companies' approaches to transparency reporting practices differ in a few substantial ways. As a result, most of the data contained in the Companies' transparency reports cannot be compared. Thus, the data has limited informative value, particularly insofar as it is difficult to draw inferences about the extent to which governments are requesting and obtaining access to data, including personal data, held by Internet-based companies.

The empirical research set out in this Report highlights the limited value of data contained in transparency reports published by the selected Companies. For example, all the Companies disclose the number of government requests they receive, so it is possible to arrive at a sector-wide number of government requests during a reporting period. However, such number, in and of itself, says nothing about the actual scale and scope of those requests. A single request may be associated with one specific subject, be it a user, an account or another identifier, but another request may have a significantly larger scope, referring to thousands of subjects. This informational gap can be overcome based on uniform reporting on the subject of the requests (e.g. number of individual records or accounts to which those requests relate) and the number of affected accounts or individuals. Regrettably, the Companies use a variety of terms to refer to the subject of the requests (e.g. "users specified", "accounts specified", "URLs affected"), and only three of them currently report numbers of affected individuals or accounts. Consequently, arriving at anything close to a reliable metric indicative of sector-wide scale and scope of government access requests is not currently possible.

Overall, given the Companies' different reporting approaches and a lack of clarity regarding exactly how they count some metrics and define certain terms, efforts should be made to standardise the content of transparency reports and thereby expand the scope for comparison and analysis.

To be sure, substantial efforts have been made to harmonise the content of transparency reports. Examples of these efforts include the *Transparency Reporting Toolkit* from New America and the Berkman Center for Internet and Society (Woolery, Budish and Bankston, 2016), New Zealand's Privacy Commissioner's 2015 Report on Transparency Reporting Trial (New Zealand Privacy Commissioner, 2015), Canada's 2015 Transparency Reporting Guidelines (Government of Canada, 2015), and the Working paper titled 'Transparency Reporting: Promoting accountability when governments access personal data held by companies', adopted at the 57th meeting of the International Working Group on Data Protection in Telecommunications in Seoul (International Working Group on Data Protection in Telecommunications, 2015). However, much of this work is either very broad (i.e. mainly setting out general principles and potential courses of action) or relevant only to a specific jurisdiction. In a world of ubiquitous transborder data flows, further work must be carried out to agree on minimum common standards for transparency reporting and terminology in order to improve comparability across companies, sectors and jurisdictions.

***Recommendation**:* Governments should work together and liaise with companies, data protection authorities, international organisations and civil society organisations to develop meaningful guidance on minimum standards for transparency reporting (including harmonising the terminology used, and standardising the data to be reported) in order to improve the potential for comparisons to be made across companies, sectors and jurisdictions. The good practices set out in Section 3 above can serve as a baseline to inform this endeavour.

Further research focusing on more jurisdictions

Agreeing on a common nomenclature, standards and metrics that can be easily compared across sectors and countries is, of course, no easy task. As the majority of the Companies surveyed in this Report are based in the US, most of the Companies' reporting practices are based on US law and are predominantly concerned with data access demands from the US Government. Companies based in other jurisdictions are subject to different laws, regulations and standards, so their reporting practices (including what they can include in their transparency reports) are bound to differ. As a matter of fact, whilst companies should ideally produce granular transparency reports about the type of government requests for user data they receive and the number of users impacted, *many countries' laws either prohibit this or are unclear about whether such disclosures are permitted*.

Therefore, more research should be conducted in order to identify similarities and disparities in reporting approaches and applicable laws across countries, this time focusing on non-US jurisdictions. This exercise would contribute to both increasing legal certainty as to which reporting practices are allowed under different countries' applicable laws and forming an adequate evidence base to inform agreement on common standards and good practices in transparency reporting.

In the aftermath of the Snowden leaks, much of the media coverage and commentary was misleading, in particular by suggesting that bulk collection of data was mainly a US and UK practice. However, empirical research has shown that bulk access is much more widespread (European Parliament, 2013; Cate and Demsey, 2017b). Against this background, not only is additional research focused on more jurisdictions necessary for the purpose of achieving greater uniformity in - and therefore enhance the informative value of – transparency reporting, but is also essential to produce a comprehensive snapshot of current practices, including the extent to which different governments are obtaining (potentially unlimited) access to personal data held by private companies. As noted in the Introduction, governments are best placed to provide an accurate and reliable picture of this issue, the UK and US governments having provided good examples on how to respond to calls for more transparency with the publication of transparency reports on the use and exercise of investigatory powers and national security authorities. Transparency reporting by governments is a necessary complement to reporting by private companies, and its widespread adoption should be encouraged.

***Recommendation**:* More research like that presented in this Report should be carried out, ideally on a per country basis, with an aim to clarify what reporting practices are allowed under different countries' applicable laws, and on this basis build a robust evidence base required to agree on minimum common standards and practices that are reliable and comparable on a both national and international level. Relatedly, to complement private companies' reporting and thereby contribute to elucidate the extent to which different governments are gaining access to user (including personal) data held by the private sector, transparency reporting by governments should be encouraged and widely adopted.

Inclusion of telecom service providers in the sample of surveyed companies

In addition to Internet-based companies such as those surveyed in this Report, the providers of communications services (i.e. traditional telephone operators, wireless operators and Internet service providers (ISPs)) also collect and store varied data about their customers. This data differs depending on the providers' service and business models, but it may include subscriber-identifying information, allocations of Internet addresses to individual users, mobile locational data, Internet connection and browsing data, telephone dialling records, and other addressing, signalling or routing information, usually time-stamped and capable of being linked to a specific user (Center for Democracy and Technology, 2011). As a result, telecom service providers around the world are common recipients of government access requests for users' data.

Indeed, many incidents of bulk collection of user data involve telecom service providers, not least because they tend to be subject to specific information access/disclosure obligations.[57] For example, in the US, a special court ordered a number of telecom service providers to disclose to the NSA, on a daily basis, metadata (i.e. number making the call, number called, time, duration) for all telephone calls handled by the carriers to, from, and within the country. The bulk disclosure orders were renewed every 90 days from 2006 to 2015, when Congress passed legislation putting an end to the practice (Cate and Demsey, 2017c, p. 8). Similarly, in Germany, telecom service providers are required to collect certain data about their customers, such as name, address, and telephone number, before the service is established. This information is sent to a databank kept by the Federal Network Agency, and other governmental agencies can make automated requests for this information from the databank (Cate and Demsey, 2017c, p. 8). In the UK, the UK Investigatory Powers Act 2016 imposes data retention mandates on telecom service providers and contemplates the issuance of 'bulk interception warrants' and 'bulk personal dataset warrants'.[58]

Telecom service providers appear, therefore, to have significant influence on the extent to which governments have access to personal data held by the private sector. Since only Internet-based companies were surveyed in this Report, such influence, as well as the legal mechanisms that support it, were not captured.

***Recommendation**:* To paint a comprehensive picture of the scale and scope of governments' access to private data held by the private sector, further research on transparency reporting should include traditional telephone operators, wireless operators and ISPs in the sample of surveyed companies.[59]

Removal of unnecessary and disproportionate barriers to transparency reporting

Section 1 of this Report explained that relevant practices and standards regarding government access to privately-held data in the context of law enforcement investigations tend to be fairly clear. However, the limits on powers and safeguards pertaining to the exercise of powers are typically less robust and transparent when government access demands are made in furtherance of foreign intelligence and national security objectives. Crucially, the scope of information that government agencies may access by access requests issued under foreign intelligence and national security investigations is usually significantly broader. In addition, national security intelligence gathering is invariably conducted in secrecy, and given that the prosecution of individuals is not always the intended or actual outcome, the veil of secrecy may never be lifted (International Working Group on Data Protection in Telecommunications, 2015).

In view of the above, laws and regulations under which government agencies are able to gain access to user data held by private entities in the context of foreign intelligence and national security investigations should ensure that there are obligations to be transparent when relying on this power to justify data access. In reality said laws and regulations usually restrict the ability of companies to provide meaningful statistics relating to government requests to gain access to user data. Section 2 of this Report explained that most companies surveyed provide imprecise – and consequently uninformative – statistics about national security requests.

Restrictions on detailed transparency reporting impede investigations into the extent to which governments are accessing user data held by private companies. This is particularly the case where such restrictions apply to national security- and foreign intelligence-related requests for user data, as bulk collection practices are reportedly common in intelligence gathering for those purposes (Cate and Dempsey, 2017a). To enhance transparency and accountability, unnecessary and disproportionate legal barriers to transparency reporting should be removed. As already noted, the difficulty here is that more granular reporting can allow an adversary to determine a state's capacity or workload regarding collection efforts. Any public facing report needs to balance these competing interests. Nonetheless, to determine what amounts to an unnecessary and disproportionate barrier, it would be ideal to receive the input from both governments and companies, the former group explaining what kind of restrictions they believe are necessary to protect the successful conduction of their state operations, and the latter indicating what time of granularity in the provision of information is required to achieve proper transparency and accountability.

Recommendation*:* Governments should engage with companies, data protection authorities, international governmental organisations, civil society organisations, and other regulatory bodies (including those in charge of administrative simplification), to debate on, encourage and ultimately facilitate the removal or at least reduction of unnecessary and disproportionate legal barriers to transparency reporting. The input from both governments (especially those with open government initiatives) and companies as to what they consider an unnecessary and disproportionate barrier should assist the execution of this task.

Annex

Annex A. List of surveyed companies

Company	*Transparency Reports available at*
Amazon	https://www.amazon.com/gp/help/customer/display.html?nodeId=GYSDRGWQ2C2CRYEF
Apple	https://www.apple.com/legal/transparency/
Automattic	https://transparency.automattic.com/information-requests/
Dropbox	https://www.dropbox.com/en_GB/transparency/reports
Facebook	https://govtrequests.facebook.com/government-data-requests/jan-jun-2019
Google	https://transparencyreport.google.com/user-data/overview?hl=en_GB
KaKao	https://privacy.kakao.com/main
LINE	https://linecorp.com/en/security/transparency/2019h1
LinkedIn	https://about.linkedin.com/transparency/government-requests-report#0
Medium	https://medium.com/transparency-report/government-requests-for-information-or-content-removal-9b23349b0e73
Meetup	http://web.archive.org/web/20190730135602/https://blog.meetup.com/inaugural-transparency-report/
Microsoft	https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report
Pinterest	https://help.pinterest.com/en-gb/guide/transparency-report-archive
Reddit	https://www.reddit.com/wiki/transparency
Snapchat	https://www.snap.com/en-GB/privacy/transparency
TikTok	https://www.tiktok.com/safety/resources/transparency-report?lang=en
Tumblr	https://www.tumblr.com/transparency
Twitter	https://transparency.twitter.com/en.html
Wickr	https://wickr.com/transparency/
Wikimedia Foundation	https://wikimediafoundation.org/about/transparency/

Annex B. Comparison of the Companies' approaches to reporting on the number, nature and outcome of the requests

Table A – Number and nature of the requests

Company	*Information contained in transparency reports regarding the **number** of data access requests from governments*	*Information contained in transparency reports regarding the **subject** of data access requests from governments*	*Information contained in transparency reports regarding **the countries from which the requests originate***	*Provision of Information in transparency reports regarding the **type of data** being sought by requests*
Amazon	Number of requests US requests are broken down by legal process type, including subpoenas, search warrants and other court orders. Amazon also reports ranges of US National Security requests.	No information	Distinction made between US requests and Non-US requests	No
Apple	Number of device requests, number of financial identifier requests, number of account requests, number of account preservation requests and number of emergency requests. At the US level, the first three types of requests are broken down by legal process type, including search warrants, wiretap orders, pen/register/trap and trace orders, other court orders and subpoenas. Ranges of US National Security requests are also reported.	Number of devices specified in the requests, number of financial identifiers specified in the requests, number of accounts specified in the requests (for both account requests and emergency requests).	Requests are broken down by country	Yes. Apple distinguishes requests that seek device information, financial identifiers, and account information. Apple also provides this information indirectly, reporting the number of account requests where only non-content data was provided, and number of account requests where content data was provided.
Automattic	Number of requests. At the US level, the total number of requests is broken down (in %) into different legal process types, including subpoenas, court	Number of sites specified.	Requests are broken down by country	No

	orders, search warrants, wiretap orders, pen register orders and emergency requests. Ranges of National Security requests (in bands of 250) are also reported.			
Dropbox	Number of requests At the US level, the total number of requests is broken down by legal process type, including search warrants, subpoenas and court orders. Also, Dropbox reports ranges of US National Security requests.	Number accounts listed in search warrants, subpoenas and court orders. Number of accounts is not specified for Non-US requests.	Requests are broken down by country.	Indirectly, as Dropbox reports the number of cases where non-content data and content data was provided.
Facebook	Number of total requests, number and % of emergency requests, number and % of legal process requests, and number of preservation requests. At the US level, the total number of requests is broken down by legal process request type, including search warrant, subpoena, Title III, Pen Register, Trap & Trace, Court Order: 18 USC 2703(d) and Court Order: Others. Also, Facebook reports ranges (in bands of 500) for Foreign Intelligence Surveillance Act (FISA) requests and National Security Letters (NSL).	Number of user/accounts requested.	Requests are broken down by country.	Facebook breaks down its national security requests into requests for content and non-content data.
Google	Number of user data disclosure requests. At the US level, the number of requests is broken down into different categories of requests, including subpoenas, search warrants, other court orders, other legal requests, emergency disclosure requests, pen register orders, wiretap orders and preservation requests. For all remaining countries, requests are divided into other legal requests, emergency disclosure requests and preservation requests from H2 2014 onwards. Also, Google reports ranges (in bands of 500) for Foreign Intelligence Surveillance Act (FISA) requests and National Security Letters (NSL).	Number of user/accounts specified in the requests.	Requests are broken down by country	No
Kakao	Number of requests The number of requests is broken down by type of request, including request for communication data, communication-restricting measure, communication confirmation data, and search and seizure warrant.	Number of accounts.	No	Indirectly, given certain types of reported requests (communication data and communication confirmation data).

LINE	Number of requests From H2 2017 the total number of requests is broken down (%) into different categories, including abuse of children, financial harm, bodily harm, illegal and harmful information, unauthorised access, intellectual property infringement and others.	Targeted contact information	Requests are broken down by country	No
LinkedIn	Number of requests for member data. At the US level, requests are broken down (%) by type of request, including subpoenas, search warrants, court orders and other. Ranges of National Security requests are also reported.	Accounts subject to requests	Requests are broken down by country	No
Medium	Number of requests for user information. Medium also reported the number of National Security demands they received.	No information	No	No
Meetup	Number of requests At the US level, requests are broken down into legal process type, including government and civil subpoenas. Meetup also reported ranges of US National Security Requests.	Number of accounts potentially affected	Distinction between US requests and Non-US requests	Indirectly, as Meetup reports the number of cases where non-content and content was disclosed.
Microsoft	Number of law enforcement requests and number of emergency requests. At the US level, Microsoft reports Foreign Intelligence Surveillance Act (FISA) Orders and National Security Letters (NSL).	Accounts/users specified in the requests	Requests are broken down by country	Indirectly, as Microsoft reports the number of cases where non-content and content was disclosed.
Pinterest	Number of requests At the US level, requests are broken down by US legal process type, including subpoenas, court orders and warrants. Also, Pinterest discloses ranges of National Security requests.	Accounts specified	Distinction between US requests and Non-US requests	No
Reddit	Number of information production requests, number of emergency requests and number of preservation requests. At the US level, Reddit breaks down the information production requests into different legal process types, including subpoenas, court orders, search warrants and real-time monitoring requests. Also, from 2019, Reddit discloses ranges of	No information	Information production requests, emergency requests and preservation requests are broken down by country as from 2015	No

	US National Security Requests, including National Security Letters (NSLs) and Foreign Intelligence Surveillance Act (FISA) orders.			
Snapchat	Number of criminal legal requests and emergency requests. US criminal legal requests are reported broken down by US legal process type, which include subpoenas, PRTT, court orders, search warrants, emergency disclosure requests, wiretap orders and summons. Snap also reports ranges of US national security requests (national security letters and FISA orders/directives).	Account identifiers	Requests are broken down by country	No
TikTok	Number of legal requests and number of emergency requests.	Number of accounts specified	Requests are broken down by country	No
Tumblr	Number of requests. US requests are broken down by type, including search warrants, subpoenas, court orders, emergency requests and other request (such as email or fax requests). Also, Tumblr reports US National Security requests.	Number of URLs affected	Requests are broken down by country	Indirectly, as Tumblr reports the number of cases where blog content and account data was produced.
Twitter	Number of government account information requests, number of account preservation requests, and number of emergency disclosure requests. At the US level, Twitter reports the percentages of account information requests broken down by legal process type, which include subpoenas, search warrants and court orders. Also, Twitter reports the number of National Security Letters (NSLs) received which are no longer subject to non-disclosure orders (which are not subject to the reporting limits in bands).	Accounts specified	Requests are broken down by country	Indirectly, as Twitter reports the % of cases where non-content information and content information was disclosed.
Wickr	Number of requests received. US requests are broken down into legal process type, including search warrants, court orders, law enforcement subpoenas, national security requests and other requests.	Accounts associated with requests received	Distinction between US requests and Non-US requests	No
Wikimedia Foundation	Number of total requests, informal government requests, legal process requests, preservation requests and emergency disclosures.	User accounts potentially affected	Government requests are broken down by country	Yes. The Wikimedia Foundation reports the % of content requests and % of non-content

	Legal process requests are reported broken down by legal process type, including, administrative subpoenas, civil subpoenas, criminal subpoenas, search warrants, court orders, international court orders and national security requests. Emergency disclosures are broken down into different types, including individual threats, terrorist threats, suicide threats, other and emergency requests.			requests.

Table B – Outcome of the requests

Company	*Company's reported response to the request*	*Breakdown of the response*	*Does the Company report the number of accounts/users impacted by the request?*
Amazon	Production of information requested.	Number of requests with full response, partial response, no response.	No
Apple	For device requests and financial identifiers requests, production of information requested. For preservation requests, preservation of data. For account requests, production of information requested (content and non-content data) and full or partial rejection of the request. For emergency requests, production of data and rejection/challenging of the request.	Number and % of device requests where data was provided. Number and % of financial identifier requests where data was provided. Number of account requests where no data was provided, number of account requests challenged in part or rejected in full, number of account requests where only non-content data was provided, number of account requests where content data was provided and % of account requests where data was provided. For preservation requests, number of accounts where data was preserved. For emergency requests, number of requests rejected/challenged & no data provided, number of requests where no data was provided, and number and % of requests where data was provided.	Yes. For account requests, number of accounts for which data was provided (until H2 2017). For preservation requests, number of accounts where data was preserved.
Automattic	Production of all or some of the information requested.	No breakdown. Only the % of requests where some or all information was produced is reported.	No
Dropbox	Provision of information requested.	Number of requests where data does not exist, no information provided, non-content data provided and content data provided (for US requests only).	Yes. Number of accounts listed in search warrants, subpoenas and court orders where data does not exist, no information provided, non-content data provided and

			content data provided (for US requests only).
Facebook	Production of information requested.	% of total requests where some data was produced, % of emergency requests where some data was produced, and % of legal process requests where some data was produced.	No
Google	Production of some data.	No breakdown. Only the % of requests where some data was produced is reported.	No
Kakao	Processing of the request.	No breakdown. Only the number of processed requests is reported.	No
LINE	Production of data.	% of handled requests and number of requests where data was provided.	No
LinkedIn	Production of data.	No breakdown. Only the % of requests for which LinkedIn provided some data is reported.	Yes. Number of accounts for which LinkedIn provided some data.
Medium	No outcome (as Medium received zero requests)	No outcome (as Medium received zero requests).	No (as Medium received zero requests).
Meetup	Disclosure of information and rejection of the request.	Number of rejected requests, requests where content was disclosed and requests where only non-content was disclosed.	No
Microsoft	Production of information and rejection of the request.	Number and % of content disclosures, number and % of non-content disclosures, number and % of requests where no data was found and number and % of rejected requests.	No
Pinterest	Production of information.	No breakdown. Only the number of total requests where information was produced is reported.	No
Reddit	Disclosure of information.	No breakdown. Only the number of information production and emergency requests where account information was disclosed is reported. For preservation requests, Reddit discloses the number of requests complied with.	Yes. For information production and emergency requests, number of user accounts affected (until 2016 and 2017, respectively).
Snapchat	Production of information.	No breakdown. Only the % of legal requests and emergency requests where some data was produced is reported.	No
TikTok	Production of information.	No breakdown. Only the % of requests where some data was produced is reported.	No
Tumblr	Production of information.	% of blog content produced, % of account data produced and % of compliance.	No
Twitter	Production of information,	For account information requests,	No

	noncompliance and partial compliance with the request.	% of requests where some information was produced, % of narrowed requests, and % of cases where content information and cases where non-content information was provided. For emergency requests, % of requests where some information was produced.	
Wickr	No response reported.	No breakdown.	No
Wikimedia Foundation	Production of information requested.	No breakdown. Only the number of total requests where information was produced is reported.	Yes. Number of user accounts actually affected.

Annex C. Profiles of the Surveyed Companies

1. Amazon

1. **Main reported figures – Number of requests during the reporting period / Subject of the request (e.g. users affected, accounts affected, URLs identified) / Outcome of the request (company's response)**

	No. of requests	Full response	Partial response	No response
H1 2015				
US requests	851	559	139	153
Non-US requests	132	108	7	17
H2 2015				
US requests	882	365	330	187
Non-US requests	78	15	3	60
H1 2016				
US requests	1,803	763	551	489
Non-US requests	120	15	24	81
H2 2016				
US requests	1,525	598	550	377
Non-US requests	58	1	1	56
H1 2017				
US requests	1,936	834	631	471
Non-US requests	75	0	2	73
H2 2017				
US requests	1,761	712	602	447
Non-US requests	103	0	0	103
H1 2018				
US requests	2,242	699	960	583
Non-US requests	290	11	1	278
H2 2018				
US requests	2,166	846	832	488
Non-US requests	216	7	0	209
H1 2019				
US requests	2,508	1,174	796	538
Non-US requests	271	1	0	270
H2 2019				
US requests	2,395	815	971	609
Non-US requests	227	5	0	222

US requests are broken down by legal process type, including subpoenas, search warrants and other court orders.

From H1 2018 onwards Amazon reports the numbers above for its Amazon Web Services branch separately.

Amazon also reports ranges of US National Security requests (bands of 250).

Full response: it means that Amazon responded to valid legal process by providing all of the information requested.

Partial response: it means that Amazon responded to valid legal process by providing only some of the information requested.

No response: it means that Amazon responded to valid legal process by providing none of the information requested.

2. Explanation of the information that can be accessed through the different legal processes / Explanation of international requests processing

Subpoenas: Amazon produces non-content information only in response to valid and binding subpoenas. Amazon does not produce content information in response to subpoenas.

Search warrants: Amazon may produce non-content and content information in response to valid and binding search warrants.

Court orders: Amazon's responses to other court orders depend on the nature of the request.

National Security requests: Amazon's responses to these requests depend on the nature of the request.

"Non-content" information means subscriber information such as name, address, email address, billing information, date of account creation, and certain purchase history and service usage information.

"Content" information means the content of data files stored in a customer's account.

Non-US requests: Amazon's responses to these requests depend on the nature of the request. A non-US law-enforcement agency seeking to obtain data from Amazon must work through the available legal and diplomatic channels in its jurisdiction, including through bi-lateral or multi-lateral legal assistance treaties ("MLATs") or letters rogatory processes. Such international requests may be made to the US Department of Justice Office of International Affairs.

Amazon objects to overbroad or otherwise inappropriate subpoenas, search warrants, court orders and non-US requests as a matter of course.

3. Reporting on user notifications

Unless it is prohibited from doing so or has clear indication of illegal conduct in connection with the use of Amazon products or services, Amazon notifies customers before disclosing content information.

4. Reporting on the products and services targeted by the requests

Amazon reports 'all requests received by Amazon' in one single group until H2 2017.

From H1 2018 onwards, Amazon reports total requests and Amazon Web Services requests separately.

Amazon does not specify which specific products and services are included in 'total requests'.

5. Frequency with which TRs are issued

On a half-yearly basis. First report covers requests for user data in H1 2015.

2. Apple

1. **Main reported figures – Number of requests during the reporting period / Subject of the request (e.g. users affected, accounts affected, URLs identified) / Outcome of the request (company's response)**

Government device requests

These are the device-based requests received from a government agency seeking customer data related to specific device identifiers, such as a serial number or IMEI number. Examples of these requests are where law enforcement agencies are working on behalf of customers who have requested assistance regarding lost or stolen devices. Additionally, Apple regularly receives multi-device requests related to fraud investigations. Device-based requests generally seek details of customers associated with devices or device connections to Apple services.

Worldwide	No. of device requests received	No. of devices specified in the requests	No. of device requests where data was provided	% of device requests where data was provided
H1 2014	20,221	281,770	12,146	60%
H2 2014	22,537	661,482	13,713	61%
H1 2015	26,996	362,794	15,957	59%
H2 2015	30,687	167,090	17,959	59%
H1 2016	30,006	261,934	20,695	72%
H2 2016	30,184	151,105	21,737	72%
H1 2017	30,814	233,052	23,856	77%
H2 2017	29,718	309,362	23,445	79%
H1 2018	32,342	163,823	25,829	80%
H2 2018	23,183	213,737	22,691	78%
H1 2019	31,778	195,577	26,051	82%

The figures above are also reported broken down by country.

Apple clarifies that one request may contain one or multiple device identifiers. For example, in a case related to the theft of a shipment of devices, law enforcement may seek information related to several device identifiers in a single request.

Government Financial Identifier Requests

These are financial identifier-based requests received from a government agency seeking customer data related to specific financial identifiers, such as credit card or gift card number. Examples of these requests are where law enforcement agencies are working on behalf of customers who have requested assistance regarding suspected fraudulent credit card activity used to purchase Apple products or services. Financial identifier-based requests generally seek details of suspected fraudulent transactions.

Worldwide	No. of financial identifier requests received	No. of financial identifiers specified in the requests	No. of financial identifier requests where data was provided	% of financial identifier requests where data was provided
H2 2016	2,392	21,249	1,821	76%
H1 2017	2,690	22,707	2,182	81%
H2 2017	3,101	24,050	2,636	85%

H1 2018	3,973	33,505	3,185	80%
H2 2018	4,626	21,034	3,547	77%
H1 2019	4,664	23,899	3,432	74%

The figures above are also reported broken down by country.

Apple clarifies that one request may contain one or multiple financial identifiers. For example, in a case related to large scale fraud, law enforcement may seek information related to several credit card numbers in a single request.

Government Account Requests

These are the account-based requests received from a government agency seeking customer data related to specific Apple account identifiers, such as Apple ID or email address. Examples of these requests are where law enforcement agencies are working on cases where they suspect an account may have been used unlawfully or in violation of Apple's terms of service. Account-based requests generally seek details of customers' iTunes or iCloud accounts, such as a name and address; and in certain instances, customers' iCloud content, such as stored photos, email, iOS device backups, contacts or calendars.

Worldwide	No. of account requests received	No. of accounts specified in the requests	No. of accounts for which data was provided	No. of account requests where no data was provided	No. of accounts requests challenged in part or rejected in full	No. of account requests where only non-content data was provided	No. of account requests where content data was provided	% of account requests where data was provided
H1 2014	1,495	2,807	1,333	661	476	678	156	56%
H2 2014	1,425	6,510	5,256	504	355	730	191	65%
H1 2015	1,667	4,472	1,884	560	401	810	297	66%
H2 2015	1,813	12,850	9,956	581	383	892	340	68%
H1 2016	2,564	12,245	7,963	224	542	1,432	414	71%
H2 2016	2,231	10,577	8,880	471	175	1,350	410	79%
H1 2017	3,020	43,836	38,643	611	262	1,082	607	80%
H2 2017	3,358	10,786	8,427	600	224	2,041	717	82%
H1 2018	4,177	40,641	--	--	320	2,391	1,006	81%
H2 2018	4,875	22,503	--	--	363	2,782	1,227	82%
H1 2019	6,480	37,605	--	--	425	3,351	1,927	85%

The figures above are also reported broken down by country.

Apple clarifies that one request may contain one or multiple account identifiers. For example, in a case related to suspected phishing, law enforcement may seek information related to several accounts in a single request. Moreover, Apple informs that it challenges requests based on grounds such as a request does not have a valid legal basis, or is unclear, inappropriate, and/or over-broad. For example, Apple may reject a law enforcement request if it considers the scope of data requested as excessively broad for the case in question.

Examples of non-content data are a subscriber, account connections or transactional information. Examples of content data are stored photos, email, iOS device backups, contacts or calendars.

Government Account Preservation Requests

Examples of such requests are where law enforcement agencies suspect an account may have been used unlawfully or in violation of Apple's terms of service, and request Apple to preserve the account data while they obtain legal process for the data.

Worldwide	No. of account preservation requests received	No. of accounts specified in the requests	No. of accounts where data was preserved
H1 2017	1,108	2,206	1,648
H2 2017	1,214	2,547	1,852
H1 2018	1,579	4,033	2,802
H2 2018	1,823	5,553	3,963
H1 2019	2,616	6,689	4,749

The figures above are also reported broken down by country.

Apple clarifies that one request may contain one or multiple account identifiers. For example, in a case related to suspected illegal activity, law enforcement may request Apple to preserve information related to several accounts in a single request.

Government Emergency Requests

Worldwide	No. of emergency requests received	No. of requests rejected/challenged & no data provided	No. of requests where no data was provided	No. of requests where data was provided	% of requests where data was provided
H1 2015	246	--	--	--	--
H2 2015	178	--	--	--	--
H1 2016	171	--	--	--	--
H1 2017	268	11	40	217	81%
H2 2017	290	9	43	238	82%
H1 2018	407	9	56	342	84%
H2 2018	494	6	41	447	90%
H1 2019	598	18	44	536	90%

The figures above are also reported broken down by country.

For the US only, Apple reports ranges (in bands of 500) for Foreign Intelligence Surveillance Act (FISA) requests and National Security Letters (NSL), including the number of requests received and number of users/accounts specified. FISA requests are broken down into content and non-content requests. Also at the US level only, Apple reports since H2 2016 the number of device requests, financial identifier requests and account requests broken down by legal process type, including search warrants, wiretap orders, pen/register/trap and trace orders, other court orders and subpoenas.

2. Indication of the legal processes required to access different types of information / Explanation of international requests processing

The type of customer data sought in requests varies depending on the case under investigation. For example, in stolen device cases, law enforcement generally seeks details of customers associated with devices or device connections to Apple services. In credit card fraud cases, law enforcement generally seeks details of suspected fraudulent transactions. Depending on what the

legal request asks, Apple will provide subscriber or transaction details in response to valid legal requests received.

In instances where an Apple account is suspected of being used unlawfully, law enforcement may seek details of the customer associated with the account, account connections or transaction details or account content. For the United States:

- Apple requires a search warrant issued upon a showing of probable cause in order to provide customer content.
- A wiretap order allows the government to obtain content on a forward-looking basis for a specific limited period of time as opposed to stored historical content. Apple can intercept users' iCloud email communications upon receipt of a valid Wiretap Order. Apple cannot intercept users' iMessage or FaceTime communications as these communications are end-to-end encrypted.
- A pen register order allows the government to obtain non-content data on a forward-looking basis for a specific limited period of time as opposed to stored historical information. A pen register order can be combined with a court order/warrant for historical records, in such instances Apple reports the process type as pen register/trap and trace order.
- Non-content data such as subscriber and transaction information can be provided in response to a court order.
- Non-content data such as device, subscriber and connection information can be provided in response to a subpoena.

The type of customer data sought in emergency situations generally relates to details of customers' connection to Apple services. An emergency request must relate to circumstances involving imminent danger of death or serious physical injury to any person. If Apple believes in good faith that it is a valid emergency, it may voluntarily provide information to law enforcement on an emergency basis

International requests for content must comply with applicable laws, including the US Electronic Communications Privacy Act (ECPA). A request under a Mutual Legal Assistance Treaty or Agreement with the United States is in compliance with ECPA.[60]

3. Reporting on user notifications

When Apple receives an account request seeking customers' information and data, it notifies the customer that it has received a request concerning their personal data except where it is explicitly prohibited by the legal process, by a court order Apple receives, or by applicable law. Apple reserves the right to make exceptions, such as instances where it believes providing notice creates a risk of injury or death to an identifiable individual, or where the case relates to child endangerment, or where notice is not applicable to the underlying facts of the case.

4. Reporting on the products and services targeted by the requests

Apple reports requests affecting 'Apple's products and services', without specifying which ones in particular.

5. Frequency with which TRs are issued

On a half-yearly basis. First report covers requests for user data in H1 2014.

3. Automattic

1. **Main reported figures – Number of requests during the reporting period / Subject of the request (e.g. users affected, accounts affected, URLs identified) / Outcome of the request (company's response)**

Worldwide	No. of requests	% of requests where some or all information was produced	No. of sites specified
H2 2013	36	33%	51
H1 2014	75	16%	85
H2 2014	32	38%	39
H1 2015	69	46%	81
H2 2015	70	39%	80
H1 2016	79	39%	159
H2 2016	85	34%	116
H1 2017	78	35%	98
H2 2017	110	29%	125
H1 2018	102	42%	121
H2 2018	116	63%	125
H1 2019	118	45%	173

The numbers above are available on a per country basis.

Also, in the US context only, the total number of requests (%) is broken down into different legal process types, including subpoenas, court orders, search warrants, wiretap orders, pen register orders and emergency requests. Ranges of National Security Requests (in bands of 250) are also reported.

Moreover, Automattic reports from H1 2016 the % of US requests accompanied with a non-disclosure order.

2. **Indication of the legal processes required to access different types of information / Explanation of international requests processing**

Automattic does not voluntarily provide governments with access to data about users (private or public) for law enforcement, intelligence gathering, or other surveillance purposes. Automattic turns over user information only upon receipt of valid US legal process. In particular, Automattic requires a search warrant before producing content information and/or user communications to government agencies/law enforcement.

In response to a valid subpoena issued by a US authority, Automattic can provide the following information, when it is available: First and last names, Phone number, Email address, Date/time stamped IP address from which a site was created, Physical address provided by the use, PayPal transaction information.

Autommatic requires a specific court order or search warrant before providing additional IP address data or information relating to a specific post or a specific comment.

Automattic responds to court judgments from the United States only, or foreign judgments specifically adopted by a United States or California court. Law enforcement agencies from outside the US may obtain a US order through the Mutual Legal Assistance Treaty (MLAT) process outlined in 28 U.S.C. § 1782 and 18 U.S.C. § 3512.

Preservation Requests from US Governmental and Law Enforcement Agencies

When a government or law enforcement agency from within the US asks that a request to preserve data remain confidential from the affected user, Automattic keeps it confidential for 45 days, with the expectation that the agency will be serving a valid US subpoena or search warrant that includes the required certification (18 U.S.C. § 2705(b)) or court-issued nondisclosure order. If a nondisclosure order is provided along with a subpoena or search warrant, Automattic will continue to keep the preservation request(s) confidential under the same conditions as the nondisclosure order for the subsequent subpoena/search warrant. If, after 45 days, law enforcement has not served a subpoena or search warrant with the required 18 U.S.C. § 2705(b)) court-issued nondisclosure order, and has not withdrawn the request for continued preservation, Automattic will then inform the user of the preservation request. In light of the October 19, 2017, Department of Justice guidance on nondisclosure orders, Automattic asks that the agency include a specific end date for the nondisclosure period in any proposed order to the court, and that any period or extensions of time last no longer than a combined total of one year.

Preservation Requests from Non-US Law Enforcement Agencies

Law enforcement agencies from outside the US may request that Automattic preserves information while the agency obtains a valid subpoena, search warrant, or court order from a court in the US, through the Mutual Legal Assistance Treaty (MLAT) process. The MLAT is a mechanism by which a foreign law enforcement agency can obtain a US court order for information pursuant to a criminal investigation, as outlined in 28 U.S.C. § 1782 and 18 U.S.C. § 3512. While Automattic may preserve information in response to requests from non-US law enforcement agencies pending the MLAT process, Automattic will not turn over any actual user or account information until Automattic receives a United States subpoena, search warrant, or court order. If, after 90 days from the date of requesting preservation, the non-US law enforcement agency has not provided documentation to Automatttic confirming that it has initiated the MLAT process, Automattic will stop preserving the data.

If the non-US law enforcement agency requests that Automattic keeps the preservation request confidential from the affected user, Automattic may do so at its discretion. Automattic will only consider such requests if the agency's request meets Automattic's criteria for authenticity, necessity, and timeliness, and only for the period of time necessary for the agency to obtain a court-issued nondisclosure order through the MLAT process described above.

3. Reporting on user notifications

Automattic's policy is to notify our users of any legal process Automattic receives regarding their account, so that they may challenge the request if they wish. The only exception is if Automattic is prohibited by law (not just asked nicely by the police) from making such a notification.

If a request for information is validly issued, Automattic will preserve the necessary information before informing the user of the request. In most cases, upon notification to the user of the request for information, that user will be provided with either 7 days or the amount of time before the information is due, whichever is later, during which time the user may attempt to quash or legally challenge the request. If, prior to the deadline, Automattic receives notice from the user that he or she intends to challenge a request for information, Automattic will not deliver any information until that process concludes. Automattic also reviews the information requests received and may lodge its own challenge to the scope or validity of the legal process received, on behalf of a user, whether or not the user pursues his/her own legal challenge.

4. **Reporting on the products and services targeted by the requests**

   Government requests 'received by Automattic' are reported, without reference to any specific product or service.

5. **Frequency with which TRs are issued**

   On a half-yearly basis. First report covers requests for user data in H2 2013.

4. Dropbox

1. **Main reported figures – Number of requests during the reporting period / Subject of the request (e.g. users affected, accounts affected, URLs identified) / Outcome of the request (company's response)**

   US legal request

	No. of requests	Accounts listed	Does not exist	No information provided	Non-content provided	Content provided	Notice provided
2012	87	--	11	5	47	24	18
2013	277	850	46	33	94	104	103
H1 2014	229	454	30	16	80	103	89
H2 2014	255	1,20	21	13	108	113	78
H1 2015	416	640	24	23	149	213	228
H2 2015	565	680	48	10	179	328	218
H1 2016	582	1,279	46	14	221	301	265
H2 2016	817	1,450	46	69	367	335	310
H1 2017	1,445	2,411	77	86	605	677	575
H2 2017	1,332	2,605	68	133	484	637	1,183
H1 2018	1,305	3,877	104	123	433	645	455
H2 2018	1,276	2,596	79	248	423	526	373
H1 2019	1,297	2,846	101	150	435	611	382

Dropbox reports the numbers above broken down by legal process type, including search warrants, subpoenas and court orders. In addition, from 2013 onwards, Dropbox reports their response (i.e. does not exist, no information provided, non-content provided, content provided, notice provided) at the account level, also broken down into search warrants, subpoenas and court orders.

Also, Dropbox reports ranges of US national security requests (in bands of 250).

Non-US requests

	No. of requests received by Dropbox	Information provided
2012	<20	0
2013	90	0
H1 2014	37	0
H2 2014	19	0
H1 2015	7	0
H2 2015	4	0

H1 2016	6	0
H2 2016	29	0
H1 2017	33	1
H2 2017	19	1
H1 2018	20	1
H2 2018	13	0
H1 2019	26	0

From H1 2014, Non-US requests are broken down by country.

2. **Indication of the legal processes required to access different types of information / Explanation of international requests processing**

   In response to valid search warrants, Dropbox may produce non-content and content information. Dropbox does not provide content information in response to subpoenas or court orders.

   At this time, Dropbox typically requires non-US governments to follow the Mutual Legal Assistance Treaty process or letters rogatory process so that a US court will issue the required US legal process to Dropbox.[61]

3. **Reporting on user notifications**

   Dropbox provides notice to its users when a government requests their information. Once Dropbox has determined that a request is valid, Dropbox usually notifies the user (unless Dropbox is legally prohibited from doing so) and respond with an encrypted copy of the information specified in the legal process. However, government requests frequently include a court-granted non-disclosure order, which prohibits Dropbox from giving notice to the affected user. In cases where Dropbox receives a non-disclosure order, Dropbox notifies the user when it has expired. Dropbox is also committed to following the USA Freedom Act. This ensures that courts have the opportunity to review non-disclosure obligations for any national security letters Dropbox may receive. Dropbox believes that services such as Dropbox should always be permitted to provide notice to affected users.

4. **Reporting on the products and services targeted by the requests**

   Not applicable.

5. **Frequency with which TRs are issued**

   On an annual basis between 2012 and 2013, on a half-yearly basis from 2014 onwards. First report covers government requests for user data in 2012.

5. Facebook

1. **Main reported figures – Number of requests during the reporting period / Subject of the request (e.g. users affected, accounts affected, URLs identified) / Outcome of the request (company's response)**

Worldwide	Total requests	% of Requests where some data was produced	Users/Accounts requested	No. and % of emergency requests	% of Emergency requests where some data was produced	No. and % of legal process requests	% of Legal process requests where some data was produced
H1 2013	25,607	62.1%	37,954				
H2 2013	28,147	63.4%	39,320				
H1 2014	34,946	61.6%	49,479				
H2 2014	35,051	61.2%	50,236				
H1 2015	41,214	64%	57,551				
H2 2015	46,710	67.9%	65,917				
H1 2016	59,229	69.9%	86,735	3K (5.1%)	76.6%	56.2K (94.9%)	69.6%
H2 2016	64,279	72.5%	93,878	4.3K (6.6%)	77.6%	60K (93.4%)	72.3%
H1 2017	78,890	74.4%	116,663	4.9K (6.2%	72.9%	74K (93.8%)	74.5%
H2 2017	82,341	74.8%	126,149	6.2K (7.5%)	78.6%	76.2K (92.5%)	74.5%
H1 2018	103,815	74%	159,874	9.2K (8.8%)	79.8%	94.6K (91.2%)	73.2%
H2 2018	110,634	73.1%	163,049	9.6K (8.6%)	73.2%	101.1K (91.4%)	73%
H1 2019	128,617	73.6%	206,294	12.2K (9.5%)	70.1%	116.4K (90.5%)	73.7%

From H1 2013 onwards the number of total requests, users/accounts requested and % of requests where some data was produced are available on a per country basis. The numbers of emergency requests and legal process requests are available on a per country basis from H1 2016 onwards.

Worldwide	Number of preservation requests	Users/accounts requested
H1 2016	38.7K	67.1K
H2 2016	45.7K	77.8K
H1 2017	58.9K	100.3K
H2 2017	57.1K	93K
H1 2018	69.1K	115.3K
H2 2018	71.4K	119.6K
H1 2019	83.2K	140.6K

Preservation requests numbers are also available on a per country basis.

Only for the US, Facebook reports the number of total requests, users/accounts requested and % of requests where some data was produced broken down by legal process request type, including search warrant, subpoena, Title III, Pen Register, Trap & Trace, Court Order: 18 USC 2703(d) and Court Order: Others. Also, Facebook reports ranges (in bands of 500) for Foreign Intelligence Surveillance Act (FISA) requests and National Security Letters (NSL), including total requests and accounts specified. FISA requests are broken down into content and non-content requests[62].

2. Indication of the legal processes required to access different types of information / Explanation of international requests processing

US legal process requirements

Facebook discloses account records solely in accordance with its terms of service and applicable law, including the United States Federal Stored Communications Act ("SCA"), 18 USC sections 2701-2712. Under US law:

- A valid subpoena issued in connection with an official criminal investigation is required to compel the disclosure of basic subscriber records (defined in 18 USC section 2703(c)(2)), which may include: name, length of service, credit card information, email address(es) and a recent login/logout IP address(es), if available.
- A court order issued under 18 USC section 2703(d) is required to compel the disclosure of certain records or other information pertaining to the account, not including contents of communications, which may include message headers and IP addresses, in addition to the basic subscriber records identified above.
- A search warrant issued under the procedures described in the United States Federal Rules of Criminal Procedure or equivalent local warrant procedures upon presentation of a probable cause is required to compel the disclosure of the stored contents of any account, which may include messages, photos, videos, Timeline posts and location information.
- Facebook interprets the national security letter provision as applied to Facebook to require the production of only two categories of information: name and length of service.

International legal process requirements

Facebook discloses account records solely in accordance with its terms of service and applicable law. A Mutual Legal Assistance Treaty request or letter rogatory may be required to compel the disclosure of the contents of an account.[63]

3. Reporting on user notifications

Facebook's policy is to notify people who use Facebook's service of requests for their information prior to disclosure, unless Facebook is prohibited by law from doing so or in exceptional circumstances, such as child exploitation cases, emergencies or when providing notice would be counter-productive. Facebook will also provide delayed notice upon expiry of a specific non-disclosure period in a court order and where it has a good-faith belief that exceptional circumstances no longer exist and it is not otherwise prohibited by law from doing so. Law enforcement officials who believe that notification would jeopardise an investigation must obtain an appropriate court order or other appropriate process establishing that providing notice is prohibited.

4. Reporting on the products and services targeted by the requests

Facebook states that its reports include information about requests related to its various products and services including Facebook, Instagram, Messenger, Oculus and WhatsApp, unless otherwise noted.

Facebook reports all the government requests it receives in the aggregate, without providing specific numbers for each product or service.

5. **Frequency with which TRs are issued**

On a half-yearly basis. First report covers requests for user data in H1 2013.

6. Google

1. **Main reported figures – Number of requests during the reporting period / Subject of the request (e.g. users affected, accounts affected, URLs identified) / Outcome of the request (company's response)**

Worldwide	No. of user data disclosure requests	No. of users/accounts specified in the requests	% of requests where data was produced
H1 2011	15,744	25,342	72%
H2 2011	18,257	28,562	70%
H1 2012	20,938	34,615	67%
H2 2012	21,389	33,634	66%
H1 2013	25,879	42,500	65%
H2 2013	27,477	42,648	64%
H1 2014	31,698	48,615	65%
H2 2014	30,140	50,587	63%
H1 2015	35,365	68,908	63%
H2 2015	40,677	81,311	64%
H1 2016	44,943	76,713	64%
H2 2016	45,550	74,074	60%
H1 2017	48,941	83,345	65%
H2 2017	48,877	87,263	66%
H1 2018	57,868	126,581	67%
H2 2018	63,149	135,302	67%
H1 2019	75,368	164,537	73%

The figures above are also available on a per country basis.

Google adds the following clarifications: "The number of user data requests we receive and numbers of accounts implicated may not be a 1:1 ratio. We err on the side of over-inclusion and report the total number of accounts requested.

A single user data request may seek information about multiple accounts, so the number of accounts requested may be higher than the number of total requests. Additionally, one person can have multiple Google Accounts, or the same account may the subject of several different requests for user information. For example, if we receive a subpoena and later a search warrant for the same account, it will be counted multiple times here."[64]

"The column for the number of "users/accounts" attempts to reflect the number of users or accounts that were subject to a government request for user information. This number is not necessarily an aggregate count of unique users for several reasons. For example, the same Gmail account may be specified in several different requests for user information, perhaps once in a subpoena and then later in a search warrant. We add both instances to the "user/accounts" total even though it's the same account. Similarly, we might receive a request for a user or account that doesn't exist at all. In that case, we would still add both the request and the non-existent account to the totals. We may also receive a request that has multiple identifiers (for example, multiple

YouTube video URLs) that resolve to the same user account. We've taken efforts to reduce over-inclusiveness, but have decided it is better to err on the side of a greater number.

We also receive requests where the information disclosed does not include specific user/account identifiers, for example, a request where the resulting information was anonymized or aggregated. In such cases, we would not count the anonymized or aggregated users/accounts in the total number."[65]

Google also reports diplomatic requests. There were 193 diplomatic requests in H1 2019.

For the US only, the number of requests is broken down into different categories of requests, including subpoenas, search warrants, other court orders, other legal requests, emergency disclosure requests, pen register orders, wiretap orders and preservation requests. For all remaining countries, requests are divided into other legal requests, emergency disclosure requests and preservation requests from H2 2014 onwards. Also, Google reports ranges (in bands of 500) for Foreign Intelligence Surveillance Act (FISA) requests and National Security Letters (NSL), including total requests and users/accounts specified. FISA requests are broken down into content and non-content requests.[66]

2. Indication of the legal processes required to access different types of information / Explanation of international requests processing

When the service provider is Google LLC, the following applies:

Requests from US government agencies in civil, administrative, and criminal cases

The Fourth Amendment to the US Constitution and the Electronic Communications Privacy Act (ECPA) restrict the government's ability to force a provider to disclose user information. US authorities must at least do the following:

- **In all cases:** Issue a subpoena to compel disclosure of basic subscriber registration information and certain IP addresses
- **In criminal cases:**
  - Get a court order to compel disclosure of non-content records, such as the To, From, CC, BCC, and Timestamp fields in emails
  - Get a search warrant to compel disclosure of the content of communications, such as email messages, documents, and photos

Requests from US government agencies in cases that involve national security

In investigations related to national security, the US government may use a National Security Letter (NSL) or one of the authorities granted under the Foreign Intelligence Surveillance Act (FISA) to compel Google to provide user information.

- An NSL doesn't require judicial authorization and can only be used to compel us to provide limited subscriber information.
- FISA orders and authorizations can be used to compel electronic surveillance and the disclosure of stored data, including content from services like Gmail, Drive, and Photos.

Requests from government authorities outside the US

Google LLC sometimes receives data disclosure requests from government authorities outside of the US. When Google receives one of these requests, Google may provide user information if doing so is consistent with all of the following:

- **US law**, which means that the access and disclosure is permitted under applicable US law, such as the Electronic Communications Privacy Act (ECPA)
- **Law of the requesting country** which means that Google requires the authority to follow the same due process and legal requirements that would apply if the request were made to a local provider of a similar service
- **International norms** which means Google only provides data in response to requests that satisfy the Global Network Initiative's Principles on Freedom of Expression and Privacy and its associated implementation guidelines
- **Google's policies** which include any applicable terms of service and privacy policies, as well as policies related to the protection of freedom of expression.

When the service provider is Google Ireland Limited, the following applies:

Requests from Irish government agencies

Google Ireland considers Irish law when evaluating requests for user information by an Irish agency. Irish law requires that Irish law enforcement authorities obtain a judicially-authorized order to compel Google Ireland to provide user information.

Requests from government authorities outside Ireland

Google Ireland offers services to users located throughout the European Economic Area and Switzerland, and Google sometimes receives data disclosure requests from government authorities outside of Ireland. In this case, Google may provide user data if doing so is consistent with all of the following:

- **Irish law**, which means that the access and disclosure is permitted under applicable Irish law, such as the Irish Criminal Justice Act
- **European Union (EU) law applicable in Ireland**, which means any EU laws applicable in Ireland including the General Data Protection Regulation (GDPR)
- **Law of the requesting country** which means that Google requires the authority to follow the same due process and legal requirements that would apply if the request were made to a local provider of a similar service
- **International norms** which means Google only provides data in response to requests that satisfy the Global Network Initiative's Principles on Freedom of Expression and Privacy and its associated implementation guidelines
- **Google's policies** which include any applicable terms of service and privacy policies, as well as policies related to the protection of freedom of expression

3. Reporting on user notifications

When Google receives a request from a government agency, Google sends an email to the user

account before disclosing information. If the account is managed by an organization, Google gives notice to the account administrator. Google does not give notice when legally prohibited under the terms of the request. Google provides notice after a legal prohibition is lifted, such as when a statutory or court-ordered gag period has expired.

Google might not give notice if the account has been disabled or hijacked. Also, Google might not give notice in the case of emergencies, such as threats to a child's safety or threats to someone's life, in which case Google provides notice if it learns that the emergency has passed.

4. **Reporting on the products and services targeted by the requests**

Google reports cases where a government agency asks Google to disclose information about someone who uses 'Google services'. Google does not specify which specific services are included in that term, but does indicate that government agencies commonly request information from Gmail, YouTube, Google Voice and Blogger.

Google reports all the government requests it receives in the aggregate, without providing concrete numbers for specific products or services.

5. **Frequency with which TRs are issued**

On a half-yearly basis. First report covers requests for user data in H1 2011.

7. Kakao

1. **Main reported figures – Number of requests during the reporting period / Subject of the request (e.g. users affected, accounts affected, URLs identified) / Outcome of the request (company's response)**

	No. of requests	No. of processed requests	No. of accounts
H1 2012	11,474	7,818	136,377
H2 2012	10,795	6,823	66,780
H1 2013	6,282	3,768	110,097
H2 2013	7,707	5,193	310,661
H1 2014	8,159	5,571	223,618
H2 2014	6,793	4,889	134,013
H1 2015	7,032	4,482	627,419
H2 2015	6,584	4,012	174,263
H1 2016	8,081	5,587	292,447
H2 2016	8,675	5,181	335,585
H1 2017	10,663	6,328	403,198
H2 2017	10,024	6,177	302,668
H1 2018	14,719	8,113	643,068
H2 2018	17,544	10,950	695,749
H1 2019	17,471	11,653	1,597,970

The numbers above are broken down by service (i.e. Daum and Kakao) and type of request, including communication data, communication-restricting measure, communication confirmation data, and search and seizure warrant.

2. **Indication of the legal processes required to access different types of information / Explanation of international requests processing**

The information that can be accessed via each type of legal process is indicated in Kakao's description of each of such processes, as detailed in the preceding section.

No information on international requests processing is provided.

3. **Reporting on user notifications**

No information available.

4. **Reporting on the products and services targeted by the requests**

Kakao reports the government requests it receives broken down into requests received by Daum and requests received by Kakao.

5. **Frequency with which TRs are issued**

On a half-yearly basis. First report covers requests for user data in H1 2012.

8. LINE

1. **Main reported figures – Number of requests during the reporting period / Subject of the request (e.g. users affected, accounts affected, URLs identified) / Outcome of the request (company's response)**

Worldwide	No. of requests	% of handled requests	Requests where data provided	Targeted contact information
H2 2016	1,719	58%	997	1,268
H1 2017	1,614	65%	1,052	1,310
H2 2017	1,390	76%	1,058	1,345
H1 2018	1,576	76%	1,190	1,560
H2 2018	1,725	76%	1,304	1,612
H1 2019	1,625	79%	1,285	1,601

The figures above are available on a per country basis.

LINE clarifies that a single request may contain multiple contact information.

"Targeted Contact Information" refers to the specific contact information (phone number, LINE ID, etc.) of users that authorities suspect are involved in crime.

The number of requests where data was provided is broken down by type of request, including warrant, investigation-related inquiry and emergency.

From H2 2017 the total number of requests is broken down (%) into different categories, including abuse of children, financial harm, bodily harm, illegal and harmful information, unauthorised access, intellectual property infringement and others.

2. **Indication of the legal processes required to access different types of information / Explanation of international requests processing**

LINE may respond to a law enforcement agency only in the case of a warrant, if there is a request for cooperation with an investigation with a legal basis (such as Investigation-Related Inquiry in Japan), and if judged that it would avert present danger (emergency).

LINE will only cooperate with criminal investigations in accordance with strict information handling rules, and only when a thorough verification confirms the legality and propriety of the investigation.

Provision of information is strictly limited to information required for the relevant investigations and trials. When internal review processes determine the law enforcement agency's request in accordance with the writ of summons, bench warrant or detention warrant is too broad for its purpose of use, LINE will ask the law enforcement agency for additional explanation, and reject the request unless it finds there are reasonable grounds. LINE does not submit information of unspecified users irrelevant to investigations. Disclosure of content generally includes the following information held by the company:

- Registered information of specified users (profile image, display name, email address, phone number, LINE ID, date of registration, etc.)
- Communication data of specified users (message delivery date, IP address of sender) – this information is not disclosed through Investigation-Related Inquiries.
- A maximum of seven days' worth of specified users' text chats - Only when end-to-end encryption has not been applied (if end-to-end encryption has been enabled, even the company cannot decrypt/extract the contents of text chats, so there is no disclosure of the contents of text chats). End-to-end encryption has applied by default since July 1, 2016. This information is disclosed only when receiving an effective warrant issued by a court. Video / picture / files / location information / phone call audio and other such data will not be disclosed.

LINE handles requests from non-Japanese law enforcement according to the Act on International Assistance, the mutual legal assistance treaties (MLATs) of relevant countries and other international investigation assistance frameworks. This includes instances where the Japanese police receive a request via the International Criminal Police Organization (ICPO) or Japan's Ministry of Foreign Affairs receives a request via an embassy.

3. Reporting on user notifications

LINE provides notification in accordance with applicable laws or ordinances and when the company otherwise deems it appropriate (ex: notification is required by foreign laws and ordinances that do not lead to greater spread of harm or injury).

4. Reporting on the products and services targeted by the requests

LINE notes that the reports prior to and including H1 2018 include data related to the LINE messaging app only. The reports for Jul-Dec 2018 and onward cover data related to all services that LINE Corporation provides. Any data from services provided by LINE subsidiaries and affiliates is not included in its reports.

LINE reports all the government requests it receives in the aggregate, without providing specific numbers for each product or service.

5. Frequency with which TRs are issued

On a half-yearly basis. First report covers requests for user data in H2 2016.

9. LinkedIn

1. **Main reported figures – Number of requests during the reporting period / Subject of the request (e.g. users affected, accounts affected, URLs identified) / Outcome of the request (company's response)**

	Requests for member data	Accounts subject to requests	Requests for which LinkedIn provided some data	Accounts for which LinkedIn provided some data
H2 2011				
US	65	84	84%	--
Globally[67]	73	97	75%	--
H1 2012				
US	64	96	79%	--
Globally	67	99	76%	--
H2 2012				
US	45	49	80%	--
Globally	48	53	75%	--
H1 2013				
US	70	84	49%	--
Globally	83	97	49%	--
H2 2013				
US	56	90	61%	--
Globally	72	110	47%	--
H1 2014				
US	85	1,069	65%	101
Globally	116	1,144	52%	150
H2 2014				
US	84	202	70%	76
Globally	100	218	60%	78
H1 2015				
US	99	141	78%	113
Globally	112	161	74%	116
H2 2015				
US	127	226	72%	134
Globally	139	238	66%	134
H1 2016				
US	128	291	68%	150
Globally	145	310	62%	153
H2 2016				
US	135	345	74%	192
Globally	150	373	73%	211
H1 2017				
US	187	594	71%	229
Globally	207	614	68%	237
H2 2017				
US	191	602	76%	331
Globally	224	642	63%	344
H1 2018				
US	196	1,077	37%	399

Globally	232	1,126	35%	419
H2 2018				
US	203	1,069	52%	553
Globally	247	1,122	41%	569
H1 2019				
US	314	1,170	82%	639
Globally	362	1,233	77%	662

Non-US government requests are available on a per country basis.

For the US only, as from H1 2013, LinkedIn provides granular information, including the number of requests, the accounts subject to requests, requests for which LinkedIn provided some data (%), subpoenas (%), search warrants (%), court orders (%), Other (%), National security requests received, and national security requests (accounts subject to request). There are two "National Security Requests" categories - one for requests received and one for accounts impacted. Such requests are reported in the aggregate and in ranges of 0 to 249, 250 to 500, and so forth.

2. Indication of the legal processes required to access different types of information / Explanation of international requests processing

Except in limited emergency situations, law enforcement agents seeking information about member accounts must be made through formal US legal procedures, such as subpoenas, court orders, and search warrants. Certain types of member data, including messages, invitations and connections, have a high bar for disclosure and can only be disclosed pursuant to a valid search warrant from an entity with proper jurisdiction.

Depending on the type of formal legal process provided, LinkedIn may be able to respond with one or more of the following types of data:

Basic Subscriber Information, which may include: Email address(es) Member identification number ("Member ID"), Date and time of account creation, Billing information, Snapshot of Member Profile Page (which may include Profile Summary, Experience, Education, Recommendations, Groups, Network Update Stream, User profile photo) and IP Logs (which may include Member ID, IP address and the date the account was accessed)

Pursuant to a valid search warrant from an entity with proper jurisdiction, LinkedIn may be able to provide **Member Content** as well as **Basic Subscriber Information**. **Member Content** may include Invitations, Messages and Connections. LinkedIn requires a search warrant to produce any Member Content responsive to law enforcement Data Requests.

Data requests from outside of the United States and the EU generally must be made through an official Mutual Legal Assistance Treaty (MLAT) or, letter rogatory.

3. Reporting on user notifications

LinkedIn's policy is to notify Members of Requests for their data unless LinkedIn is prohibited from doing so by statute or court order. Law enforcement officials who believe that notification would jeopardize an investigation should obtain an appropriate court order or other valid legal process that specifically precludes Member notification, such as an order issued pursuant to 18 U.S.C. §2705(b). When a Request is accompanied by a nondisclosure order, LinkedIn will notify the affected Member(s) as soon as the order is overturned or expires on its own terms.

4. Reporting on the products and services targeted by the requests

Not applicable.

5. **Frequency with which TRs are issued**

   On a half-yearly basis. First report covers government requests for user data in H2 2011.

10. Medium

1. **Main reported figures – Number of requests during the reporting period / Subject of the request (e.g. users affected, accounts affected, URLs identified) / Outcome of the request (company's response)**

   Medium reported the number of government requests for user information received during the reporting period: 0

   Medium also reported the number of National Security demands they received, including national security letters and orders issued by the Foreign Intelligence Surveillance Court: 0 in each case.

2. **Indication of the legal processes required to access different types of information / Explanation of international requests processing**

   Non-public, non-content information about Medium users will be released to law enforcement only in response to appropriate legal process such as a subpoena, court order, or other valid legal process — or in response to a valid emergency request.

   Contents of communications (e.g., post drafts and photos) will be released only in response to a valid search warrant from an agency with proper jurisdiction over Medium.

   Emergency disclosure requests: Medium evaluates emergency disclosure requests on a case-by-case basis in compliance with relevant US law (e.g., 18 U.S.C. § 2702(b)(8)). If Medium receives information that gives Medium a good faith belief that there is an exigent emergency involving the danger of death or serious physical injury to a person, Medium may provide information necessary to prevent that harm, if available.

   Mutual legal assistance treaties: A Mutual Legal Assistance Treaty (MLAT) defines how the United States and another country will help each other in legal matters such as criminal investigations. Through an MLAT, a foreign government can ask the US government for help in obtaining evidence from entities in the United States, including companies like Medium. If the US government approves the request, Medium would respond to it. Medium's policy is to promptly respond to requests that are issued via US court either by way of a MLAT or letters rogatory upon proper service of process.

3. **Reporting on user notifications**

   Medium's policy is to notify users of requests for their account information and provide a copy of the request prior to disclosure unless Medium is prohibited from doing so (e.g., Medium receives an order under 18 U.S.C. § 2705(b)).

   Exceptions to prior notice may include exigent or counterproductive circumstances (e.g., emergencies or account compromises).

   In cases in which Medium is not permitted to give a user prior notice, Medium will provide post-disclosure notice to the user unless legally prohibited from doing so.

4. **Reporting on the products and services targeted by the requests**

   Not applicable.

5. **Frequency with which TRs are issued**

   In principle, on an annual basis. However, Medium has issued only one TR, covering year 2014.

11. Meetup

1. **Main reported figures – Number of requests during the reporting period / Subject of the request (e.g. users affected, accounts affected, URLs identified) / Outcome of the request (company's response)**

	No. of requests	No. of accounts potentially affected	Rejected	Content disclosed	Only non-content disclosed
2016					
US requests	9	8	4	3	2
International requests	1	1	0	0	1

   'Potentially Affected' refers to the number of accounts, groups, or events that would be affected if Meetup complied completely with each request (not including data requests that did not specify enough information to identify a target).

   "Rejected" means the total number of requests pushed back on for any reason (e.g., overbroad, did not specify enough information to identify a target).

   "Content" is information concerning the substance or meaning of a particular communication, which can include text of emails, messages, and more. Content disclosures may also include non-content information.

   "Non-Content" is account information that is not considered to be content, which can include basic subscriber information such as the name used to create an account, the internet protocol address from which the account was created, or the internet protocol address used to sign in to an account, along with dates and times. Non-content information can also include more detailed transactional data about a user's communications such as the internet protocol addresses, email addresses, handles, or phone numbers that sent or received the communications, as well as when the communications occurred, how long in duration, and how large in size they were.

   US requests are broken down into government and civil subpoenas. Meetup also reported ranges of US National Security Requests.

   Moreover, Meetup reported the number of requests with non-disclosure orders, the number of cases where there was no non-disclosure order and notice was provided, and the number of cases where there was no non-disclosure order and notice was not provided.

2. **Indication of the legal processes required to access different types of information / Explanation of international requests processing**

   No information available.

3. Reporting on user notifications

There is no explicit statement on Meetup's policy on this matter. However, as seen above, Meetup disclosed cases where notice was provided and cases where notice was not provided. Therefore, it can be inferred that Meetup's policy is to notify users unless prohibited from doing so.

4. Reporting on the products and services targeted by the requests

Not applicable.

5. Frequency with which TRs are issued

In principle, on an annual basis. However, Meetup has issued only one TR, covering year 2016.

12. Microsoft

1. Main reported figures – Number of requests during the reporting period / Subject of the request (e.g. users affected, accounts affected, URLs identified) / Outcome of the request (company's response)

Law enforcement requests

Worldwide	Total No. of requests	Accounts/users specified in the request	No. and % of Content disclosures	No. and % of non-content disclosures	No. and % of requests where no data was found	No. and % of rejected requests
H1 2013	37,196	66,539	817 2.2%	28,698 77.2%	6,769 18.2%	911 2.4%
H2 2013	35,083	58,676	815 2.32%	26,811 76.43%	6,263 17.85%	1,194 3.4%
H1 2014	34,494	58,562	903 2.62%	25,916 75.13%	5,638 16.34%	2,037 5.91%
H2 2014	31,002	52,997	1,043 3.36%	22,685 73.18%	4,932 15.91%	2,342 7.55%
H1 2015	35,228	62,750	1,084 3.08%	23,822 67.62%	5,939 16.86%	4,383 12.44%
H2 2015	39,083	64,614	957 2.45%	25,780 65.96%	7,230 18.5%	5,116 13.09%
H1 2016	35,572	60,372	943 2.65%	23,445 65.91%	6,637 18.66%	4,547 12.87%
H2 2016	25,837	44,976	946 3.66%	16,621 64.33%	4,255 16.47%	4,015 15.54%
H1 2017	25,367	44,831	1,101 4.34%	15,971 62.96%	4,076 16.07%	4,219 16.63%
H2 2017	22,939	40,181	901 3.93%	14,073 61.35%	3,972 17.32%	3,993 17.41%
H1 2018	23,222	46,488	1,069 4.60%	14,261 61.41%	4,144 17.85%	3,748 16.14%
H2 2018	21,433	41,112	1,267 5.91%	13,165 61.42%	3,290 15.35%	3,711 17.31%

H1 2019	24,175	43,727	1,301 5.38%	12,909 53.40%	3,496 14.46%	6,469 26.76%

The numbers above are available on a per country basis.

In the US context, Microsoft reports Foreign Intelligence Surveillance Act (FISA) Orders and National Security Letters (NSL), providing ranges (in bands of 1,000 until H2 2014, bands of 500 afterwards) of orders seeking disclosure of content, accounts impacted by orders seeking content, orders seeking disclosure of only non-content, and accounts impacted by non-content orders.

Emergency requests

Worldwide	Total No. of emergency requests	Accounts/users specified in the request	No. and % of Content disclosures	No. and % of non-content disclosures	No. and % of requests where no data was found	No. and % of rejected requests
H1 2017	183	279	15 8.2%	100 54.64%	38 20.77%	30 16.39%
H2 2017	139	242	14 10.07%	70 50.36%	23 16.55%	32 23.02%
H1 2018	195	300	10 5.13%	120 61.54%	34 17.44%	31 15.90%
H2 2018	227	303	12 5.29%	135 59.47%	47 20.70%	33 14.54%
H1 2019	363	581	21 5.79%	206 56.75%	79 21.76%	57 15.70%

The numbers above are available on a per country basis.

2. Indication of the legal processes required to access different types of information / Explanation of international requests processing

Microsoft produces data in response to valid legal requests from governmental entities in countries where Microsoft Corporation is located. Microsoft requires an official, signed document issued pursuant to local law and rules. Specifically, Microsoft requires a subpoena or equivalent before disclosing non-content, and only disclose content to law enforcement in response to a warrant (or its local equivalent). Microsoft's compliance team reviews government demands for customer data to ensure the requests are valid, rejects those that are not valid, and only provides the data specified in the legal order.

Non-content data include basic subscriber information, such as email address, name, state, country, ZIP code, and IP address at time of registration. Other non-content data may include IP connection history, an Xbox gamertag, and credit card or other billing information. Conversely, content is what Microsoft's customers create, communicate, and store on or through Microsoft's services, such as the words in an email exchanged between friends or business colleagues or the photographs and documents stored on OneDrive or other cloud offerings such as Office 365 and Azure.

Emergency requests: In limited circumstances Microsoft may disclose information to criminal law enforcement agencies where Microsoft believes the disclosure is necessary to prevent an emergency involving danger of death or serious physical injury to a person. Each request is carefully evaluated by Microsoft's compliance team before any data is disclosed, and the

disclosure is limited to the data that Microsoft believes would enable law enforcement to address the emergency. Some of the most common emergency requests involve suicide threats and kidnappings.

3. **Reporting on user notifications**

Microsoft gives prior notice to users whose data is sought by a law enforcement agency or other governmental entity, except where prohibited by law. Microsoft may withhold notice in exceptional circumstances, such as emergencies where notice could result in danger (e.g., child exploitation investigations), or where notice would be counterproductive (e.g., where the user's account has been hacked). Microsoft also provides delayed notice to users upon expiration of a valid and applicable nondisclosure order unless Microsoft, in its sole discretion, believes that providing notice could result in danger to identifiable individuals or groups or be counterproductive.

4. **Reporting on the products and services targeted by the requests**

Government requests 'received by Microsoft' are reported, without reference to any specific product or service.

5. **Frequency with which TRs are issued**

On a half-yearly basis. First report covers government requests for user data in H1 2013.

13. Pinterest

1. **Main reported figures – Number of requests during the reporting period / Subject of the request (e.g. users affected, accounts affected, URLs identified) / Outcome of the request (company's response)**

US government requests

Quarter	No. of requests	Requests where information was produced	Accounts specified	Accounts notified
Q3 2013	7	--	7	--
Q4 2013	5	--	5	--
Q1 2014	7	--	7	--
Q2 2014	9	--	19	--
Q3 2014	10	--	15	--
Q4 2014	13	--	19	--
Q1 2015	9	9	13	4
Q2 2015	19	17	25	13
Q3 2015	11	11	13	5
Q4 2015	7	7	7	2
Q1 2016	6	6	6	1
Q2 2016	18	15	35	3
Q3 2016	20	17	84	77
Q4 2016	26	25	32	6
Q1 2017	78	74	86	40
Q2 2017	42	40	44	13
Q3 2017	23	22	24	5
Q4 2017	12	10	10	1

Q1 2018	12	10	11	4
Q2 2018	12	11	12	6
Q3 2018	20	18	28	9
Q4 2018	13	13	14	2
Q1 2019	19	19	20	7
Q2 2019	28	25	30	10
Q3 2019	34	34	44	9
Q4 2019	15	15	18	7

Accounts notified means that the account owner was notified before the disclosure of information.

US government requests are broken down by US legal process type, including subpoenas, court orders and warrants.

Also, Pinterest discloses ranges (in bands of 250) of National Security requests.

Non-US. Government information requests

Quarter	No. of requests	Requests where information was produced	Accounts specified
Q3 2013	0	--	0
Q4 2013	0	--	0
Q1 2014	1	--	1
Q2 2014	1	--	3
Q3 2014	0	--	0
Q4 2014	0	--	0
Q1 2015	0	0	0
Q2 2015	0	0	0
Q3 2015	0	0	0
Q4 2015	0	0	1
Q1 2016	0	0	0
Q2 2016	0	0	0
Q3 2016	0	0	0
Q4 2016	0	0	0
Q1 2017	0	0	0
Q2 2017	0	0	0
Q3 2017	0	0	0
Q4 2017	0	0	0
Q1 2018	0	0	0
Q2 2018	0	0	0
Q3 2018	1	1	2
Q4 2018	0	0	0
Q1 2019	0	0	0
Q2 2019	0	0	0
Q3 2019	0	0	0
Q4 2019	3	3	4

2. Indication of the legal processes required to access different types of information / Explanation of international requests processing

For US law enforcement agencies

To compel Pinterest to provide a user's information, a valid subpoena, court order or search warrant is required. To compel Pinterest to provide a user's content, a valid search warrant must be obtained.

For non-US law enforcement agencies

Non-US law enforcement agencies must obtain a valid US court order (via the mutual legal assistance treaties or letter rogatory).

3. **Reporting on user notifications**

Pinterest's policy is to notify users of law enforcement requests by providing them with a complete copy of the request before producing their information to law enforcement agencies. Pinterest may make exceptions to this policy if:

- Pinterest is legally prohibited from providing notice (e.g. by an order under 18 U.S.C. § 2705(b))
- an emergency situation exists involving a danger of death or serious physical harm to a person or place
- Pinterest has reason to believe that notice would not go to the actual account holder (e.g. an account has been hijacked or an email address is invalid)

If Pinterest receives a National Security Letter (NSL) from the US government that includes an indefinite non-disclosure order, Pinterest's policy is to ask the government to seek judicial review of the order pursuant to the USA FREEDOM Act.

In cases where notice is not provided because of a court order or emergency situation, Pinterest's policy is to provide notice to the user once the court order or emergency situation has expired.

4. **Reporting on the products and services targeted by the requests**

Not applicable.

5. **Frequency with which TRs are issued**

On a quarterly basis. First report covers government requests for user data in Q3 2013.

14. Reddit

1. **Main reported figures – Number of requests during the reporting period / Subject of the request (e.g. users affected, accounts affected, URLs identified) / Outcome of the request (company's response)**

	No. of information production requests	No. of requests where account information was turned over	No. of user accounts affected
2014			
US requests	43	28	66
Foreign requests	5	0	0

2015			
US requests	62	49	131
Foreign requests	14	1	2
2016			
US requests	112	98	--
Foreign requests	19	0	--
2017			
US requests	152	125	--
Foreign requests	24	0	--
2018			
US requests	319	285	--
Foreign requests	28	0	--
2019			
US requests	372	322	--
Foreign requests	34	7	--

Foreign information production requests are broken down by country as from 2015.

At the US level only, Reddit breaks down the information production requests into different legal process types, including subpoenas, court orders, search warrants and real-time monitoring requests. Also, from 2019, Reddit discloses ranges (in bands of 250) of US National Security Requests, including National Security Letters (NSLs) and Foreign Intelligence Surveillance Act (FISA) orders.

In the 2014 TR, Reddit also reported the No. of requests with legally binding gag orders (13).

	No. of emergency requests	No. of requests where account information was turned over	No. of user accounts affected
2014			
US requests	7	4	7
Foreign requests	--	--	--
2015			
US requests	15	4	4
Foreign requests	7	5	5
2016			
US requests	19	3	3
Foreign requests	19	3	3
2017			
US requests	41	10	--
Foreign requests	14	5	5
2018			
US requests	207	146	--
Foreign requests	27	16	--
2019			
US requests	296	251	--
Foreign requests	70		--

Foreign emergency requests are broken down by country as from 2015.

Worldwide	No. of preservation requests received	No. of preservation requests complied with
2015	20	18
2016	41	34
2017	79	59
2018	171	155
2019	224	192

Foreign preservation requests are available on a per country basis as from 2015.

2. Indication of the legal processes required to access different types of information / Explanation of international requests processing

Reddit requires a subpoena if a government wants Reddit to share basic subscriber information, which includes IP addresses, the date that an account was created and e-mail addresses.

Reddit requires a court order for any non-content information with respect to a user's account, aside from basic subscriber information. This may include a user's preferences, message headers and any other information Reddit has on a user that is "non-content".

Reddit requires a search warrant based on probable cause to disclose user content information, such as private messages and posts/comments (including those that have been deleted or otherwise hidden from public view, if the information is reasonably accessible to Reddit). Most content is publicly available without Reddit's assistance, and Reddit objects to such requests, accordingly.

Preservation requests: A preservation request may result in information being retained beyond its standard retention period. In accordance with the ECPA, Reddit will only preserve user account information for a period of up to 90 days, and will not disclose the information to law enforcement unless and until Reddit receives legal process. After the 90-day period lapses, Reddit purges the preserved data unless it receives a preservation extension request (at which point Reddit will preserve the account information for an additional 90 days).

Emergency Disclosure Requests: Reddit may disclose limited user information to law enforcement/government entities if Reddit has a good faith belief that an emergency exists involving the imminent threat of death or serious physical injury to a person, and disclosure is required without delay. Reddit evaluates these requests on a case-by-case basis.

International Requests: Reddit is a US-based company. As such, Reddit will not turn over user information in response to a formal request by a non-US government unless a US court requires it.

3. Reporting on user notifications

Reddit's policy is to notify users (to the extent legally permissible) of any request for information received with respect to their account if, after comprehensive evaluation of the request, Reddit determines that it is required to disclose or remove content.

Many requests Reddit receives contain demands to withhold notice from users that carry no legal weight. Reddit actively contests or disregards these non-binding demands. Where Reddit receives an order to delay or refrain from notice for a defined period of time, Reddit will endeavour to provide notice to the user after expiration of that time period if Reddit has reason to believe that the circumstances giving rise to the nondisclosure order no longer present the risk of an adverse result.

Reddit does not give users notice if it receives a preservation request with respect to their account, as a preservation request, alone, does not compel Reddit to disclose information to authorities.

4. **Reporting on the products and services targeted by the requests**

Not applicable.

5. **Frequency with which TRs are issued**

On an annual basis. First report covers requests for user data in 2014.

15. Snapchat

1. **Main reported figures – Number of requests during the reporting period / Subject of the request (e.g. users affected, accounts affected, URLs identified) / Outcome of the request (company's response)**

	Criminal legal requests / Other requests[68]	Account identifiers	% of requests where some data was produced	Emergency requests	Account identifiers	% of requests where some data was produced
1 Nov 2014 – 28 Feb 2015						
US requests	355	645	87%	20	21	85%
International requests[69]	--	--	--	--	--	--
H1 2015						
US requests	723	1,243	82%	38	43	82%
International requests	73	93	0%	17	24	76%
H2 2015						
US requests	796	1,736	74%	66	83	70%
International requests	66	85	0%	22	24	82%
H1 2016						
US requests	1,400	2,377	78%	72	78	82%
International requests	85	87	0%	41	51	63%
H2 2016						
US requests	1,912	3,083	77%	96	120	69%
International requests	137	175	0%	64	95	73%
H1 2017						
US requests	3,492	6,156	77%	234	278	78%
International requests	205	281	0%	123	142	68%
H2 2017						
US requests	4,738	8,092	82%	356	436	83%
International requests	304	374	0%	193	206	81%

H1 2018						
US requests	6,480	11,423	76%	755	885	77%
International requests	424	669	1%	211	247	67%
H2 2018						
US requests	6,027	10,277	77%	801	911	69%
International requests	469	667	0%	400	477	71%
H1 2019						
US requests	8,955	14,748	71%	1,106	1,310	65%
International requests	625	917	0%	665	812	63%

'Account identifiers' refers to the number of identifiers (e.g. username, email address, phone number, etc.) specified by law enforcement in legal proceedings when requesting user information. Some legal proceedings may include more than one identifier. In some instances, multiple identifiers may identify a single account. In instances where a single identifier is specified in multiple requests, each instance is included.

International requests are reported on a per country basis.

US criminal legal requests are reported broken down by US legal process type, which include subpoenas, PRTT, court orders, search warrants, emergency disclosure requests, wiretap orders and summons.

Snap also reports ranges of US national security requests (national security letters and FISA orders/directives), including number of request and account identifiers.

2. Indication of the legal processes required to access different types of information / Explanation of international requests processing

Basic subscriber information: it is collected when a user creates a new Snapchat account, alters information at a later date, or otherwise interacts with the Snapchat app. Basic subscriber information may include Snapchat username, Email address, Phone number, Display name, Snapchat account creation date and IP address, Timestamp and IP address of account logins and logouts. Basic subscriber information can be obtained through a subpoena (including one issued by a grand jury), administrative subpoena, or civil investigative demand pursuant to 18 U.S.C. § 2703(c)(2); a court order issued in accordance with 18 U.S.C. § 2703(d); or a federal or state search warrant.

Logs of Previous Snaps, Stories, and Chats: Logs contain metadata about a user's Snaps, Stories, and Chats, but not the user's content. Logs of previous Snaps, Stories, and Chats can be obtained pursuant to a court order under 18 U.S.C. § 2703(d) or a federal or state search warrant.

Location Data: it may be available for a Snapchat user who has turned on location services on their device and opted into location services in the app settings. Location data, to the extent available, can be obtained pursuant to a federal or state search warrant.

Content: Because Snap's servers are designed to automatically delete most user content, and because much of a user's content is encrypted, Snap often cannot retrieve user content except in very limited circumstances. Memories content may be available until deleted by a user. My Eyes Only content is encrypted, and although Snap can provide the data file, Snap has no way to decrypt the data. Content, to the extent available, can be obtained pursuant to a federal or state search warrant.

International Legal Process Requirements: Non-US governmental and law enforcement agencies must rely on the mechanics of the Mutual Legal Assistance Treaty ("MLAT") or letters rogatory processes to seek user information from Snap. As a courtesy to international law enforcement, Snap will review and respond to properly submitted preservation requests while the MLAT or letters rogatory process is undertaken. Also, Snap may, at its discretion, provide limited user account information to government agencies outside of the United States on an emergency basis when Snap believes that doing so is necessary to prevent death or serious physical harm to someone.

3. **Reporting on user notifications**

Snap's policy is to notify affected Snapchat users when Snap receives legal process seeking their records, information, and content. Before Snap responds to the legal process, Snap allows affected users seven days to challenge the legal process in court and to provide Snap a file-stamped copy of the challenge.

However, Snap does not provide such user notice when: (1) providing notice is prohibited by a court order issued under 18 U.S.C. § 2705(b) or by other legal authority; or (2) Snap believes an exceptional circumstance exists, such as cases involving child exploitation or the threat of imminent death or bodily injury.

4. **Reporting on the products and services targeted by the requests**

Not applicable.

5. **Frequency with which TRs are issued**

On a half-yearly basis. First report covers government requests for user data between 1 November 2014 and 28 February 2015. Subsequent reports cover six-month periods, starting on 1 January 2015.

16. TikTok

1. **Main reported figures – Number of requests during the reporting period / Subject of the request (e.g. users affected, accounts affected, URLs identified) / Outcome of the request (company's response)**

Worldwide	No. of legal requests	No. of emergency requests	No. of total requests	No. of accounts specified	% of requests where some data was produced
H1 2019	250	48	298	529	28%

The figures above are reported broken down by country.

2. **Indication of the legal processes required to access different types of information / Explanation of international requests processing**

The following information may be available in response to an enforceable law enforcement request:

- **Subscriber Information** User account information is collected when a user registers a new account or otherwise revises applicable fields within the application ("Account Information"). Account Information may include: Username, First and last name, Email address, Phone

number, Device Model, Account creation date and IP address used upon account creation. This information can be obtained through a valid subpoena (administrative, grand jury or trial), a court order issued pursuant to 18 U.S.C. 2703 (d) or a warrant.

- **Video Content:** The TikTok app allows users to create and upload videos ("Videos"). These videos may either be saved privately ("Private Videos") or posted to the TikTok app and made available to registered users ("Public Videos"). Unless an account has been set to private or the Public Video has been deleted by the user, Public Videos are available to law enforcement through the TikTok app and are therefore not provided via a Data Request. This information is available only pursuant to a warrant.
- **User Interactions:** The TikTok app allows users to interact with each other through comments to videos, direct messages, and live chats. This information is available only pursuant to a warrant.
- **Log Data:** TikTok retains logs which may include metadata regarding account logins and logouts, user generated content (e.g., file creation and modification dates), and in-app communications (e.g., to/from and timestamp information). The logs do not include the actual content of any user generated files or in-app communications. This information is available pursuant to a court order under 18 U.S.C. § 2703(d) or a warrant.

International governmental authorities should use a Mutual Legal Assistance Treaty ("MLAT") request or letters rogatory process to seek user information from TikTok.

3. **Reporting on user notifications**

In submitting a request for data concerning a particular user, law enforcement officials should note whether notification of the user would jeopardize the underlying investigation. TikTok will honour a law enforcement request not to notify the user under such circumstances.

Furthermore, if a request places TikTok on notice of an ongoing or prior violation of its terms, TikTok will take action to prevent further abuse, including account termination and other actions that may notify the user that TikTok is aware of their misconduct. If a law enforcement agency believes in good faith that taking such actions will jeopardize the ongoing investigation, it may request that TikTok defer such action in its request, and TikTok will take that request under advisement. It is the responsibility of the requesting law enforcement official to make this request.

4. **Reporting on the products and services targeted by the requests**

Not applicable.

5. **Frequency with which TRs are issued**

On a half-yearly basis. First report covers requests for user data in H1 2019.

17. Tumblr

1. **Main reported figures – Number of requests during the reporting period / Subject of the request (e.g. users affected, accounts affected, URLs identified) / Outcome of the request (company's response)**

	No. of requests	No. of URLs affected	% of blog content produced	% of account data produced	% of compliance	% of non-disclosure orders
2013						
US	407	476	31%	84%	84%	29%
International	55	53	0%	20%	20%	--
H1 2014						
US	117	218	29%	89%	89%	37%
International	17	15	0%	35%	65%	--
H2 2014						
US	173	247	34%	83%	83%	43%
International	24	22	4%	38%	38%	--
H1 2015						
US	173	211	31%	88%	88%	56%
International	17	16	0%	24%	24%	--
H2 2015						
US	188	3,792	43%	87%	87%	63%
International	27	27	0%	7%	7%	--
H1 2016						
US	237	340	38%	93%	93%	
International	37	44	0%	8%	8%	--
H2 2016						
US	215	260	32%	95%	95%	58%
International	43	57	0%	5%	5%	--

US requests are broken down by type, including search warrants, subpoenas, court orders, emergency requests and other request (such as email or fax requests).

International requests are available on a per country basis.

“Account data” includes the registration email address, how long the Tumblr account has been registered, the IP addresses used when logging in, and the IP addresses used when posting.

“Blog content” refers to the media and caption of public or private posts, as well as any messages sent between users.

Tumblr clarifies that in cases when it produced blog content, it also produced account data. Thus, the “Blog Content Produced” category is a small subset of the “Account Data Produced” category.

Non-disclosure orders: it means that a court legally prohibited Tumblr from notifying its users about the request.

Also, Tumblr reports ranges of National Security requests (bands of 250).

2. Indication of the legal processes required to access different types of information / Explanation of international requests processing

Under US law, Tumblr may disclose limited account data in response to a lawful subpoena. Account data includes registration email address, how long a Tumblr account has been registered, and login IP addresses. Account data does not include posts made to a blog, whether public or private. Because Tumblr does not collect real names or addresses, Tumblr does not and cannot

provide this information in response to a subpoena.

Tumblr may disclose the same account data described above, as well as blog content, in response to a lawful search warrant. Blog content includes the posts made to a blog, both public and private. Posts can be any of Tumblr's seven post types, and comprise both the media and the caption of any given post.

If Tumblr receives a lawful 2703(d) order, it may disclose the same account data described above, plus an additional category of account data: the IP address used to make a particular post.

In accordance with US law, Tumblr may respond to requests for disclosure of non-public information from foreign law enforcement agencies when issued by way of a US court (such as through a letter rogatory or mutual legal assistance treaty).

3. **Reporting on user notifications**

Tumblr's standard policy is to notify users of any requests for their account information prior to disclosing it to the requesting agency, so the user has an opportunity to challenge the request in court. Tumblr notes that if users were not notified prior to the disclosure of their account data, it was for at least one of the following reasons:

- The request was combined with a binding non-disclosure order;
- Notice was not practicable due to the threat of death or serious injury; or
- The case presented a serious threat to public safety.

Tumblr brakes down the cases where it complied at least in part with requests for user information into different categories of investigations, including bullying/harassment, invasion of privacy, national security and cybercrime, suicide, violent crimes, other investigations, and harm to minors. Percentages of cases where notice was given and not given are disclosed in each category.

4. **Reporting on the products and services targeted by the requests**

Not applicable.

5. **Frequency with which TRs are issued**

On a half-yearly basis. First report covers government requests for user data in 2013. Subsequent reports cover 6-month periods, starting in H1 2014. From H1 2017 Tumblr no longer issues TRs on government user data requests. Rather, Tumblr's numbers are reported in the aggregate with all requests received by Oath's brands, including Yahoo and AOL.

18. Twitter

1. **Main reported figures – Number of requests during the reporting period / Subject of the request (e.g. users affected, accounts affected, URLs identified) / Outcome of the request (company's response)**

Account information requests

Worldwide	Government account information requests	% of requests where some data was produced	Accounts specified
H1 2012	849	63%	1,181

H2 2012	1,009	57%	1,433
H1 2013	1,157	55%	1,697
H2 2013	1,410	50%	2,121
H1 2014	2,058	52%	3,131
H2 2014	2,871	52%	7,144
H1 2015	4,363	58%	12,711
H2 2015	5,560	64%	12,176
H1 2016	5,676	69%	13,152
H2 2016	6,062	64%	11,417
H1 2017	6,448	60%	11,115
H2 2017	6,268	55%	16,861
H1 2018	6,904	56%	16,882
H2 2018	6,904	56%	11,112
H1 2019	7,300	48%	12,519

The figures above are also available on a per country basis.

Twitter clarifies that 'Accounts specified' include Twitter and Periscope[70] accounts identified in government requests Twitter has received. This number may include duplicate accounts or requests for accounts that do not exist or were misidentified. This number does not include multiple identifiers associated with one account within one request (e.g., if a request contains an email address and the associated @username, Twitter counts them as one account identified).

% of requests where some information produced is defined as the percentage of legal requests where Twitter produced some or all of the information requested, for some or all of the accounts specified. For example, if Twitter was successful in narrowing the scope of information sought by the requester in the legal request, Twitter would consider this as an instance where some (but not all) of the information requested was produced.

Narrowed requests

Twitter observes that when possible, it attempts to narrow requests for account information or pushes back on the request in its entirety due to various circumstances (e.g., nature of the crime, invalid requests, requests for content with the incorrect legal process). The % of narrowed requests represents the percentage of cases out of all requests received where Twitter either did not comply with the request or partially complied.[71] This percentage includes cases in which Twitter did not provide any account information due to a push-back on the request or the account not existing, or Twitter succeeded in narrowing the request and only provided a limited subset of the requested account information (e.g., only provided basic subscriber information (BSI) when the request asked for BSI and contents of communications).

Worldwide	% of narrowed requests
H1 2016	36%
H2 2016	39%
H1 2017	42%
H2 2017	45%
H1 2018	46%
H2 2018	46%
H1 2019	52%

Content vs Non-content

Of the % of cases where some data was produced, Twitter has reported the % of cases where non-content information and content information[72] has been disclosed.

Worldwide	Non-content information	Content information
H1 2016	89%	11%
H2 2016	88%	11%
H1 2017	90%	10%
H2 2017	93%	7%
H1 2018	--	--
H2 2018	--	--
H1 2019	--	--

At the US level only, Twitter reports the percentages of account information requests broken down by legal process type, which include subpoenas, search warrants and court orders. Also, Twitter reports the percentages of account information requests under seal (i.e. where there is a court order prohibiting Twitter from notifying affected users or anyone else about the request prior to disclosure, or local law prohibits Twitter from providing notice), requests where user notice was provided (i.e. the requests in which Twitter attempted to notify the affected users prior to disclosure), and requests not under seal and no notice provided (cases where no data was disclosed in response to the request, for example, the request was withdrawn prior to disclosure or the request was defective).

Moreover, **also in the US context only**, Twitter reports the number of National Security Letters (NSLs) received which are no longer subject to non-disclosure orders (which are not subject to the reporting limits in bands), broken down into 'number of NSLs – government initiated review' (i.e. the number of National Security Letters received during the reporting period for which the US government initiated their internal review processes, determined the non-disclosure order was no longer justified or necessary, and accordingly notified Twitter that the gag order was lifted) and 'number of NSLs – provided requested review' (i.e. the number of National Security Letters received during the reporting period for which Twitter notified the government of a request for judicial review of the non-disclosure order, and the gag order was lifted).[73]

Account preservation requests

Worldwide	Government account preservation requests	Accounts specified
H1 2016	1,283	3,311
H2 2016	1,157	2,257
H1 2017	1,128	2,514
H2 2017	1,119	2,238
H1 2018	3,602	1,369
H2 2018	3,970	1,514
H1 2019	1,380	2,738

From H2 2016, the numbers above are available on a per country basis.

Twitter clarifies that the number of account preservation requests does not include preservation extension requests. Also, Twitter observes that while it does not actually turn over any information in response to these requests, reporting the volume of preservation requests and the accounts affected provides additional transparency about the types of requests Twitter receives. It also provides insight into the potential volume of requests to disclose user data that Twitter may receive in the future.

Emergency disclosure requests

Examples of some of the types of emergency requests Twitter receives include threats of self-harm and terrorism-related threats.

Worldwide	Government emergency disclosure requests	Percentage where some information was produced	Accounts specified
H1 2016	1,155	--	--
H2 2016	1,145	69%	1,479
H1 2017	1,105	64%	1,488
H2 2017	1,158	54%	1,549
H1 2018	1,580	56%	2,095
H2 2018	1,538	50%	1,811
H1 2019	1,477	57%	1,696

From H2 2016, the numbers above are available on a per country basis.

2. Indication of the legal processes required to access different types of information / Explanation of international requests processing

Requests for Twitter account information

Requests for user account information from law enforcement should be directed to Twitter, Inc. in San Francisco, California or Twitter International Company in Dublin, Ireland. Twitter responds to valid legal process issued in compliance with applicable law.

Private information requires a subpoena or court order

Non-public information about Twitter users will not be released to law enforcement except in response to appropriate legal process such as a subpoena, court order, or other valid legal process – or in response to a valid emergency request.

Contents of communications requires a search warrant

Requests for the contents of communications (e.g., Tweets, Direct Messages, photos) require a valid search warrant or equivalent from an agency with proper jurisdiction over Twitter.

Mutual legal assistance treaty (MLAT) requests

MLAT requests may authorize district courts within the United States to order Twitter to produce account information for use in a proceeding in a foreign or international tribunal, including criminal investigations. Twitter may also receive US requests for information on behalf of foreign governments based on other forms of cross-jurisdictional assistance. For example, requests may be issued pursuant to letters rogatory, or under mutual legal assistance agreements with countries that have not yet been officially brought into force through an actual treaty. Or, MLAT requests may be issued under multilateral treaties which the United States has signed and ratified, like the Inter-American Convention on Mutual Legal Assistance of the Organization of American States, the Budapest Convention on Cybercrime, or the United Nations Convention against Transnational Organized Crime.[74]

International Cooperation

US numbers in the account information requests include requests received from US Legal Attachés stationed in various international locations, who may have submitted requests under US law in part to assist their local counterparts. This type of cross-border cooperation is most likely to happen in emergency circumstances (such as those following terrorist attacks).

The CLOUD Act: the CLOUD Act (enacted in March 2018) establishes a framework for the US government to enter into bilateral agreements with certain qualifying foreign governments. Once such a bilateral agreement goes into effect, US providers may receive compulsory legal demands directly from foreign government entities to disclose account information and content of communications, as well as real-time surveillance orders (akin to PRTT and wiretap orders as described in our US report). More information about the CLOUD Act is available in a white paper recently published by the US Department of Justice. The US and UK governments have signaled that they are nearing the final negotiations for the first of these bilateral agreements. Twitter continues to closely monitor developments related to cross-border legal requests for user data.

3. **Reporting on user notifications**

Twitter's policy is to notify users of requests for their Twitter or Periscope account information, which includes a copy of the request, as soon as Twitter is able (e.g., prior to or after disclosure of account information) unless Twitter is prohibited from doing so (e.g., an order under 18 U.S.C. § 2705(b)). Twitter asks that any non-disclosure provisions include a specified duration (e.g., 90 days) during which Twitter is prohibited from notifying the user. Exceptions to user notice may include exigent or counterproductive circumstances, such as emergencies regarding imminent threat to life, child sexual exploitation, or terrorism.

4. **Reporting on the products and services targeted by the requests**

Twitter reports specific figures for its services Vine and Periscope as from H1 2016, including the total number of information requests each received, and the percentage of cases where information was disclosed. Twitter clarifies that the Requests for Vine and Periscope account information are included in the Twitter's total number of government requests. As from H1 2017, Twitter also reports the number of Vine and Periscope accounts specified in the requests.

5. **Frequency with which TRs are issued**

On a half-yearly basis. First report covers requests for user data in H1 2012.

19. Wickr

1. **Main reported figures – Number of requests during the reporting period / Subject of the request (e.g. users affected, accounts affected, URLs identified) / Outcome of the request (company's response)**

Reporting period	Type of request received	No. of requests received	Accounts associated with requests received	Response rate	Accounts receiving notice of request
26 June 2012 – 25 February 2013	US request	0	0	0	--
	Non-US request	<10	<10	0	--
January 2013 – 1 August 2013	US request	0	0		--

	Non-US request	<10	<10	0	--
January 2013 – December 2013	US request	0	0	0	--
	Non-US request	<10	<10	0	--
31 December 2013 – 1 April 2014	US request	<10	<10	0	--
	Non-US request	<10	<10	0	--
1 April 2014 – 1 October 2014	US request	2	6	--	--
	Non-US request	0	0	--	--
1 October 2014 – 25 March 2015	US request	0	0	--	--
	Non-US request	0	0	--	--
Q2 2015	US request	5	21	--	--
	Non-US request	0	0	--	--
Q3 2015	US request	2	3	--	--
	Non-US request	0	0	--	--
Q4 2015	US request	2	2	--	--
	Non-US request	0	0	--	--
H1 2016	US request	45	94	--	2
	Non-US request	1	3	--	0
H2 2016	US request	72	108	--	2
	Non-US request	3	10	--	0
H1 2017	US request	78	181	--	12
	Non-US request	6	12	--	0
1 July 2017 – 31 December 2018	US request	68	98	--	0
	Non-US request	4	6	--	0
H2 2018	US request	83	103	--	3
	Non-US request	5	6	--	0
H1 2019	US request	115	163	--	0
	Non-US request	4	4	--	0
H2 2019	US request	99	170	--	8
	Non-US request	18	25	--	0

US requests are broken down into legal process type, including search warrants, court orders, law enforcement subpoenas, national security requests and other requests.

2. Indication of the legal processes required to access different types of information / Explanation of international requests processing

Private Information Requires a Subpoena or Court Order. Non-public information about Wickr users' accounts will not be released to law enforcement except in response to appropriate legal process such as a subpoena, court order, or other valid legal process.

Contents of Communications Are Not Available. Requests for the contents of communications require a valid search warrant from an agency with proper jurisdiction over Wickr. However, Wickr's response to such a request will reflect that the content is not stored on Wickr's servers or that, in very limited instances where a message has not yet been retrieved by the recipient, the content is encrypted data which is indecipherable.

Emergency disclosure requests: Wickr may provide information to law enforcement in response to a valid emergency disclosure request. Wickr reviews emergency disclosure requests on a case-by-case basis and evaluate them under applicable law (e.g., 18 U.S.C. § 2702). If Wickr receives information that gives Wickr a good-faith belief that there is an exigent emergency involving the danger of death or serious physical injury to a person, Wickr may provide information to law

enforcement to prevent that harm, if available.

Preservation requests: Upon receipt of a valid preservation request from law enforcement under applicable law, Wickr will temporarily preserve the relevant account records for 90 days pending service of legal process. Wickr will only disclose preserved records upon receipt of valid legal process.

Mutual Legal Assistance Treaties: Wickr's policy is to promptly respond to requests that are issued via US court upon proper service of process either by way of a mutual legal assistance treaty or letter rogatory. As a courtesy to international law enforcement agencies, Wickr will review and respond to properly submitted preservation requests while the MLAT or letters rogatory process is underway.

3. **Reporting on user notifications**

Wickr's policy is to notify users of requests for their account information prior to disclosure including providing user with a copy of the request, unless Wickr is prohibited by law from doing so or if there is danger of death or serious physical injury. As soon as legally permitted to do so, Wickr will notify its users of requests for their information.

4. **Reporting on the products and services targeted by the requests**

Not applicable.

5. **Frequency with which TRs are issued**

Normally on a half-yearly basis. First report covers government requests for user data between 26 June 2012 and 25 February 2013.

20. Wikimedia Foundation

1. **Main reported figures – Number of requests during the reporting period / Subject of the request (e.g. users affected, accounts affected, URLs identified) / Outcome of the request (company's response)**

Worldwide	Total No. of requests [75]	Informal government request	Legal process requests	Information produced	User accounts potentially affected / actually affected	User accounts notified	% of Content requests	% of Non-content requests	Preservation requests	Emergency disclosures
July 2012 – June 2014	56	15	13	8	69 / 11		--	--	--	--
H2 2014	n/a[76]	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
H1 2015	23	6	2	0	28 / 0	--	--	--	--	--
H2 2015	25	7	4	1	54 / 1	--	--	--	--	--
H1 2016	13	6	0	0	14 / 0	0	0%	100%	--	--
H2	13	5	2	1	12,258	0	0%	100%	1	19

2016					/ 1					
H1 2017	18	4	4	3	23 / 3	0	0%	100%	1	16
H2 2017	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
H1 2018	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a	n/a
H2 2018	25	9	6	4	6,722 / 6,674	0	0%	100%	2	13
H1 2019	25	8	6	4	95,898 / 0	0	0%	100%	6	23

The total number of requests is reported broken down by country.

Legal process requests are reported broken down by legal process type, including, administrative subpoenas, civil subpoenas, criminal subpoenas, search warrants, court orders, international court orders and national security requests.

How Wikimedia Foundation responds to the requests (i.e. information produced) is broken down into 'partial' and 'all' as from H1 2016.[77]

Emergency disclosures are broken down into different types, including individual threats, terrorist threats, suicide threats, other and emergency requests.

'Information produced': means that as a result of a legal process (such as a subpoena) that was legally valid, some or all of the nonpublic user information requested by that legal process was produced by the Wikimedia Foundation to the requesting party. "Information produced" also applies to rare emergency situations where the Wikimedia Foundation voluntarily disclose personal information to law enforcement, or produce such information in response to an emergency request, in order to prevent imminent bodily harm or death.

'User accounts potentially affected': this number represents the number of unique user accounts implicated by requests for user data and whose data would have been disclosed if the Wikimedia Foundation had granted every request it received. This number may not reflect the number of unique individuals implicated by requests for user data, since an individual may have multiple accounts across all Wikimedia projects, and the Wikimedia Foundation record each user account separately. As a result, this number might overestimate the number of individuals implicated by user data requests.

'User accounts actually affected' This number represents the number of unique user accounts whose nonpublic information was disclosed as a result of the Wikimedia Foundation receiving a valid request for user data. This number may not reflect the number of unique individuals whose data was disclosed as a result of a valid request for user data, since an individual may have multiple accounts across all Wikimedia projects, and the Wikimedia Foundation records each user account separately. As a result, this number might overestimate the number of individuals implicated by user data requests.

An "emergency disclosure" includes two types of disclosures: voluntary disclosures, and emergency requests (see Section 3). "Voluntary disclosure" refers to a case in which the Wikimedia Foundation becomes aware of statements on the projects that threaten harm to the user who made the statements and/or other individuals, and—on the Wikimedia Foundation's initiative—choose to disclose nonpublic user information to a law enforcement agency. Such disclosures are rare; they are made only in accordance with the exceptions outlined in the

Wikimedia Foundation's Privacy Policy, such as to protect you, the Wikimedia Foundation, and others from imminent and serious bodily harm or death.

2. Indication of the legal processes required to access different types of information / Explanation of international requests processing

In some transparency reports there is a distinction made between "content" and "non-content" information. This distinction comes from the Electronic Communications Privacy Act, or ECPA (18 U.S.C. § 2703 et seq.). "Content information" refers to the contents of user communications. "Non-content" information refers to data about those communications. One common (if imperfect) analogy for explaining this is the difference between letters and envelopes. The information visible on the outside of an envelope, such as routing information, is considered non-content information. On the Wikimedia projects, this might include user agent information, IP addresses, or email addresses. The letter inside the envelope, however, is considered content information. On the Wikimedia projects, one example would be information on a Wikipedia page, which is already public. Because of the public nature of the projects, the Wikimedia Foundation very rarely receive requests for content information.

Regardless of who is requesting user data—be it an individual, a government, or a law enforcement officer—the Wikimedia Foundation only discloses nonpublic user information in accordance with its Terms of Use, Privacy Policy, and applicable US law, including the Electronic Communications Privacy Act (ECPA) (18 U.S.C. §§2510-2522, 18 U.S.C. §§ 2701-2711, and 18 U.S.C. §§ 3121-3127). The Wikimedia Foundation typically does not produce information as a result of a request unless the Wikimedia Foundation has received proper legal process. Requests must be legally valid and enforceable under United States law, in the form of a court order, subpoena, warrant, or request served under the mutual legal assistance treaty or letters rogatory process.

The Wikimedia Foundation may disclose information in response to emergency requests in accordance with ECPA (18 U.S.C. 2702(b)(8)) when there is a credible and imminent threat of death or serious bodily harm. These requests must meet specific criteria, including detailing the nature of the emergency, why it is believed to be imminent, and the specific information requested and how it is necessary to prevent the threat from being carried out.

If the Wikimedia Foundation receives a preservation request, the Wikimedia Foundation is legally required to retain the specific information indicated. However, the Wikimedia Foundation will not turn this information over to the requesting party unless they subsequently obtain a legal order, such as a subpoena or warrant, for the information in question. The Wikimedia Foundation will never produce information in response to a preservation request.

The Wikimedia Foundation requires requests originating from outside of the United States to follow the mutual legal assistance treaty (MLAT) process or letters rogatory process, so that a US court will issue the required US legal process to the Wikimedia Foundation. The MLAT process involves a network of treaties between countries, which require them to aid each other in obtaining information used for enforcing laws. Letters rogatory are a type of request issued by a court in one country to a court in another country, usually seeking assistance to serve process or gather evidence.

3. Reporting on user notifications

When the Wikimedia Foundation receives a request, the Wikimedia Foundation will notify and provide a copy of the request to the affected user(s) at least 10 calendar days before the Wikimedia Foundation discloses the requested information, provided that (1) the Wikimedia Foundation has contact information for the affected user(s); (2) disclosing the request will not create or increase a credible threat to life, limb or other serious crime; and (3) the Wikimedia Foundation is not

otherwise prohibited by law or an order from a US court of competent jurisdiction, such as an order issued pursuant to 18 U.S.C. § 2705(b), from doing so. If the Wikimedia Foundation is unable to provide information about the request to affected users because disclosing it would create a credible threat to life, limb or other serious crime; or the Wikimedia Foundation is prohibited by law, the Wikimedia Foundation will provide information about the request to affected users that the Wikimedia Foundation has contact information for within a reasonable period after the threat or legal restriction has terminated.

Upon notification to the affected user(s), the user(s) will generally be provided at least 10 calendar days before the Wikimedia Foundation will disclose the requested information (assuming the Wikimedia Foundation finds the request to be otherwise valid), during which time the affected user(s) may attempt to quash or otherwise legally challenge the request. If, prior to the disclosure, the Wikimedia Foundation receives notice from the affected user(s) that he or she intends to challenge the request, no information will be delivered until that legal challenge is resolved.

4. Reporting on the products and services targeted by the requests

Government requests 'received by the Wikimedia Foundation' are reported, without reference to any specific Wikimedia project.

5. Frequency with which TRs are issued

On a half-yearly basis. The first report covers requests for user data in the period July 2012 – June 2014; reports cover 6-month periods thereafter.

References

Access Now, EFF et. al. (2014), International Principles on the Application of Human Rights to Communications Surveillance, https://en.necessaryandproportionate.org/text

Birkinshow, P. (2006), Freedom of Information and Openness: Fundamental Human Rights?

Cate, F. and J. Dempsey (2017a), "Introduction and Background", in Bulk Collection: Systematic Government Access to Private-Sector Data

Cate, F. and J. Demsey (2017b), Bulk Collection: Systematic Government Access to Private-Sector Data, Oxford University Press

Cate, F. and J. Demsey (eds.) (2017c), Systematic Government Access to Private-Sector Data, a Comparative Analysis, Oxford University Press

Center for Democracy and Technology (2013), We Need to Know, https://cdt.org/insights/we-need-to-know/

Center for Democracy and Technology (2011), Data Retention Mandates: A Threat to Privacy, Free Expression and Business Development, https://www.cdt.org/files/pdfs/CDT_Data_Retention_Long_paper.pdf

European Parliament (2013), Study into National Programmes for Mass Surveillance of Personal Data in EU Member States and Their Compatibility with EU Law, http://www.statewatch.org/news/2013/oct/ep-study-national-law-on-surveillance.pdf

Gidari, A. (2007), Companies Caught in the Middle: Legal Responses to Government Requests for Customer Information, Univ. of San Francisco L. Rev

Government of Canada (2015), Transparency Reporting Guidelines, https://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf11057.html

International Working Group on Data Protection in Telecommunications (2015), Working paper on Transparency Reporting: Promoting accountability when governments access personal data held by companies, https://www.garanteprivacy.it/documents/10160/4809998/Working+paper+on+transparency+reporting

New America (2017), Case Study #3: Transparency Reporting, https://www.newamerica.org/in-depth/getting-internet-companies-do-right-thing/case-study-3-transparency-reporting/

New Zealand Privacy Commissioner (2015), Transparency Reporting Trial: Aug-Oct 2015, Full Report, https://privacy.org.nz/assets/Files/Reports/OPC-Transparency-Reporting-report-18-Feb-2016.pdf

OECD (2016), Ministerial Declaration on the Digital Economy ("Cancún Declaration"), https://www.oecd.org/sti/ieconomy/Digital-Economy-Ministerial-Declaration-2016.pdf

OECD (2011), Recommendation of the Council on Principles for Internet Policy Making, https://www.oecd.org/sti/ieconomy/49258588.pdf

Office of the United Nations High Commissioner for Human Rights (2014), The right to privacy in the digital age, A/HRC/27/37

Rubinstein, I., G. Nojeim and R. Lee (2014), Systematic Government Access to Personal Data: A Comparative Analysis

Telecommunications Industry Dialogue (2017), Annual Report 2016-2017, http://www.telecomindustrydialogue.org/wp-content/uploads/Industry-Dialogue-2016-17-Annual-Report.pdf

Woolery, L., R. Budish and K. Bankston (2016), "The Transparency Reporting Toolkit: Survey and Best Practice Memos for Reporting on U.S. Government Requests for User Information", Report by New America and the Berkman Center for Internet & Society, https://www.newamerica.org/oti/policy-papers/transparency-reporting-toolkit-reporting-guide-and-template/

Notes

[1] It must be noted that company transparency reports are incapable of depicting the 'full picture' of the extent to which governments access privately-held data, as governments may obtain said data from sources outside legal processes. On account of the availability of other means by which governments may access user data, only government disclosures can provide an accurate and reliable view of how and under what specific mechanisms they do so.

[2] Monthly average users (MAU) or indicative market shares were relied upon to determine which services are 'most widely used'. See Annex A 'Global Top 50 Most Popular Online Content-Sharing Services' to OECD, 'Current Approaches to Terrorist and Violent Extremist Content Among the Global Top 50 Online Content-Sharing Services', OECD Digital Economy Papers, August 2020 No. 296.

[3] See e.g. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/728110/35962_R_APS_CCS207_CCS0418538240-1_Transparency_Report_2018_print.pdf and https://www.dni.gov/files/CLPT/documents/2019_ASTR_for_CY2018.pdf

[4] These include, for example, topics such as climate change, conflict minerals and sexual harassment, exploitation and abuse.

[5] This mostly holds in common law jurisdictions, although a similar mechanism is found in civil law countries such as France, Germany and Italy.

[6] See for example European parliament Study, *National Programmes for Mass Surveillance of Personal Data in EU Member States and Their Compatibility with EU Law* (October 2013), http://www.statewatch.org/news/2013/oct/ep-study-national-law-on-surveillance.pdf; see also country reports (Chapters 2 to 14) in Bulk Collection: Systematic Government Access to Private-Sector Data, edited by Fred H. Cate and James X. Dempsey (Oxford University Press, 2017).

[7] See, for example, Global Network Initiative, Data Beyond Borders: Mutual Legal Assistance in the Internet Age, January 2015.

[8] The GNI guidance states that participating companies should disclose to users "what generally applicable government laws and policies require the participating company to provide personal information to government authorities, unless such disclosure is unlawful" and "what personal information the participating company collects, and the participating company's policies and procedures for responding to

government demands for personal information." https://globalnetworkinitiative.org//implementationguidelines/index.php

[9] For example, both Twitter and Automattic complain in their transparency reports of the restrictions to transparency reporting on national security requests imposed by US law. See https://transparency.twitter.com/en/countries/us.html and https://transparency.automattic.com/national-security/

[10] President Obama's Review Group offered quite specific recommendations for progress in this area "Legislation should be enacted authorizing telephone, Internet, and other providers to disclose publicly general information about orders they receive directing them to provide information to the government. Such information might disclose the number of orders that providers have received the broad categories of information produced, and the number of users whose information has been produced. In the same vein, we recommend that the government should publicly disclose, on a regular basis, general data about the orders it has issued in programs whose existence is unclassified." President's Review Group on Intelligence and Communications Technologies (2014, p.18) http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

[11] Access Now maintains a compilation here: www.accessnow.org/pages/transparency-reporting-index.

[12] However, the Companies use different terminologies to refer to these requests. Details are discussed later in this subsection.

[13] Amazon, Apple, Automattic, Dropbox, Facebook, Google, Kakao, LinkedIn, Meetup, Pinterest, Reddit, Snapchat, Tumblr, Twitter, Wickr and the Wikimedia Foundation.

[14] Apple, Facebook, Google, Reddit, Twitter and the Wikimedia Foundation.

[15] Apple, Facebook, Google, Microsoft, Reddit, Snapchat, TikTok, Tumblr, Twitter and the Wikimedia Foundation.

[16] Amazon, Apple, Automattic, Dropbox, Facebook, Google, LinkedIn, Medium, Meetup, Microsoft, Pinterest, Reddit, Snapchat, Tumblr, Twitter, Wickr and the Wikimedia Foundation.

[17] See Section 1 of the Reddit, Snapchat, Microsoft, Facebook, TikTok and Twitter profiles in Annex C.

[18] Kakao and Medium.

[19] Apple, Automattic, Dropbox, Facebook, Google, LINE, LinkedIn, Microsoft, Reddit, Snapchat, TikTok, Tumblr, Twitter and the Wikimedia Foundation.

[20] Amazon, Meetup, Pinterest and Wickr.

[21] Apple, Automattic, Dropbox, Facebook, Google, Kakao, LINE, LinkedIn, Meetup, Microsoft, Pinterest, Snapchat, TikTok, Tumblr, Twitter, Wickr and the Wikimedia Foundation.

[22] See column '*Information contained in transparency reports regarding the* ***subject*** *of data access requests from governments'* in Table A featured in Annex B.

[23] Apple and the Wikimedia Foundation.

[24] Dropbox, Kakao, Meetup, Microsoft, Tumblr and Twitter.

[25] See column '*Provision of Information in transparency reports regarding the* ***type of data*** *being sought by requests'* in Table A featured in Annex B.

[26] See below in this Section discussion under heading "Frequency with which Transparency Reports are issued".

[27] For example, a 5% increase in the number of requests from the United States relative and 5% decrease in the number of requests from France relative to the preceding reporting period.

[28] See below in this Section discussion under heading 'Indication of the legal processes required to access different types of information / Explanation of international requests processing'.

[29] Content data refers to the content of communications, such as private messages, posts and comments, whereas non-content data, also known as 'transactional', 'connection' or 'envelope' data, includes (a) communication attributes such as the time, duration and medium of communication, the technical parameters of the transmission devices and software, the identities and physical location of the parties and their electronic addresses; and (b) subscriber data such as name, phone number and credit card information.

[30] For example, Production Orders (Canada), Tribunal Orders (New Zealand), Requisition or Judicial Rogatory Letters (France), Solicitud de Datos (Spain), Ordem Judicial (Brazil), Auskunftsersuchen (Germany), Obligation de dépôt (Switzerland), 個人情報の開示依頼 (Japan) and Personal Data Request (United Kingdom).

[31] On MLAT processes, see the subsection "Indication of the legal processes required to access different types of information / Explanation of international requests processing under Section 2.

[32] That is the case of Facebook, Apple and Google, all of which are established in Ireland.

[33] See Section 1 of the Companies' Profiles in Annex C for the indication and description, if available, of the subjects of the requests.

[34] See http://www.justice.gov/iso/opa/resources/366201412716018407143.pdf.

[35] Under the first two reporting structures, companies can share the number of NSLs, FISA orders for content, and the number of FISA orders for non-content with which a company had to comply in bands of either 1000 (Structure 1) or 500 (Structure 2). The same bands can be used to report on 'customer selectors targeted' in each of those requests. Under Structure 3, a company may report on the aggregate number of orders with which it had to comply and also the aggregate number of customer selectors targeted by those orders, each in bands of 250. The data reported under Structures 1, 2, and 3 is subject to an 18-month delay and can be reported semi-annually. Under Structure 4, companies can report in bands of 100; however, NSLs and FISA orders must be aggregated, customer selectors targeted by those orders also must be reported in aggregate, and reporting can be at intervals no shorter than one year. Liz Woolery, Ryan Budish and Kevin Bankston, "The Transparency Reporting Toolkit: Survey & Best Practice Memos for Reporting on U.S. Government Requests for User Information", 2016 Report by New America and the Berkman Center for Internet & Society, at 104-105, available at https://www.newamerica.org/oti/policy-papers/transparency-reporting-toolkit-reporting-guide-and-template/

[36] See Section 1 of Wickr's profile in Annex C for more information on numbers of requests.

[37] Amazon, Automattic, Dropbox, Facebook, Google, LINE, LinkedIn, Pinterest, Reddit, Snapchat, TikTok, Tumblr and the Wikimedia Foundation.

[38] Apple, Meetup, Microsoft and Twitter.

[39] Automattic, Google, Kakao, LinkedIn, Pinterest, Reddit, Snapchat, TikTok, Wickr and the Wikimedia Foundation.

[40] Apple and Twitter.

[41] Apple, Dropbox, LinkedIn, Reddit and the Wikimedia Foundation.

[42] Amazon, Apple, Automattic, Dropbox, Facebook, Google, LinkedIn, Medium, Microsoft, Pinterest, Reddit, Snapchat, TikTok, Tumblr, Twitter, Wickr and the Wikimedia Foundation.

[43] For example, Google and Twitter.

[44] Dropbox, LinkedIn, Pinterest, Reddit and TikTok.

[45] Automattic, Google and Twitter.

[46] The most notable exceptions being Google, Twitter and the Wikimedia Foundation.

[47] See https://www.dropbox.com/en_GB/transparency/reports

[48] Dropbox, Meetup, Pinterest, Tumblr, Twitter, Wickr and the Wikimedia Foundation.

[49] Apple, Automattic, Microsoft, and Wikimedia Foundation.

[50] See Section 5 of Wickr's profile in Annex C.

[51] See https://www.verizonmedia.com/transparency/index.html.

[52] Twitter addresses this reality with its 'narrowed requests' metric, which represents the percentage of cases out of all requests received where Twitter either did not comply with the request or partially complied, including cases in which Twitter did not provide any account information due to a push-back on the request or the account not existing, or Twitter succeeded in narrowing the request and only provided a limited subset of the requested account information (e.g., only provided basic subscriber information (BSI) when the request asked for BSI and contents of communications). See Section 1 of Twitter's profile in Annex C.

[53] A good example is Automattic, which specifically details that a US subpoena is required for the disclosure of first and last names, phone number, email address, data/time stamped IP address from which a site was created, physical address provided by the user, and PayPal transaction information, and a court order or search warrant to provide additional IP address data or content information (such as posts or comments).

[54] See the subsection "Indication of the legal processes required to access different types of information / Explanation of international requests processing under Section 2.

[55] A strong example of such a clear policy is that of Pinterest:

"[O]ur policy is to notify users of Law Enforcement Requests by providing them with a complete copy of the request before producing their information to law enforcement. We may make exceptions to this policy where:

we are legally prohibited from providing notice (e.g. by an order under 18 U.S.C. § 2705(b));

an emergency situation exists involving a danger of death or serious physical injury to a person;

we have reason to believe notice wouldn't go to the actual account holder (e.g. an account has been hijacked)

In cases where notice isn't provided because of a court order or emergency situation, our policy is to provide notice to the user once the court order or emergency situation has expired.

See https://help.pinterest.com/en-gb/article/law-enforcement-guidelines.

[56] Twitter's approach to reporting in this area stands out for its comprehensiveness and instructional character. See Section 1 of Twitter's profile in Annex C.

[57] As a matter of fact, U.S telecom providers have been issuing transparency reports for some time. See e.g. Comcast's transparency reports, available at https://corporate.comcast.com/press/public-policy/transparency

[58] UK Investigatory Powers Act, Parts 4, 6 and 7, available at http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted.

[59] Again, governments are best positioned to elucidate the extent of their access to user data. For example, the Canadian government, bound by its Criminal Code, publishes valuable information on wiretaps in its annual reports on the use of electronic surveillance. See https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/lctrnc-srvllnc-2018/index-en.aspx

[60] Requests received from a foreign government pursuant to the MLAT process or through other cooperative efforts with the United States government are included in Apple's TRs. Apple identified 11 MLAT requests for information that were issued by the United States government in H1 2019. However, this may not be the precise number of MLAT requests received, as in some instances a United States court order or search warrant may not indicate that it is the result of an MLAT request. In instances where the originating country was identified, Apple counts and reports the MLAT request under the country of origin. In instances where the originating country was not identified, Apple counts and reports the request under the United States of America.

[61] For example, in H1 2019 Dropbox received 5 requests pursuant to mutual legal assistance treaties in place between the United States and foreign countries. The legal process received represented requests from Germany, Sweden, Canada, the Netherlands and Australia. These requests were included in Dropbox's reporting on domestic (i.e. US) requests.

[62] Non-content information/data is information such as name, length of service, credit card information, email address(es), and a recent login/logout IP addresses and other transactional information, not including the contents of communications (e.g., message headers and IP addresses).

[63] Requests received through the MLAT process are included in Facebook's reports. Facebook is unable to identify the precise number of requests it received through this channel since they result in the issuance of a search warrant or court order under US law and do not always indicate that they are the product of an MLAT request.

[64] https://transparencyreport.google.com/user-data/overview?hl=en_GB

[65] https://support.google.com/transparencyreport/answer/9713961

[66] Non-content requests implicate metadata, such as the 'from' and 'to' in email headers or the IP addresses associated with a particular account. Conversely, a content request implicates content held in a user's account, such as Gmail messages, documents, photos and videos on YouTube.

[67] US plus Non-US requests

[68] International non-emergency requests are referred to as 'Other requests' in Snapchat's reports.

[69] For this reporting period, only aggregate data was reported: 28 international requests, 35 account identifiers and 21% of requests where some data was produced.

[70] Vine was included from H1 2016 to H2 2018.

[71] Twitter informs that it may not comply with requests for a variety of reasons. For example: Twitter may not comply with requests that fail to identify a Twitter and/or Periscope account or other content on those platforms; Twitter may seek to narrow requests that are overly broad; Users may have challenged the requests after Twitter has notified them; Twitter sought additional context from the requester and did not receive a response; in other cases, Twitter may challenge the request formally through litigation or informally through discussion directly with government entities.

[72] Non-content information includes basic subscriber information (e.g., email address and phone number associated with the account) and transactional information (e.g., the to/from of a DM). While content information includes the contents of communication associated with an account (e.g, Tweet content, DM content, Vines, Periscope broadcasts). Obtaining content requires a higher legal standard like a search warrant with a showing of probable cause and a judge's signature.

[73] The numbers do not include NSLs for which Twitter requested judicial review but a court determined there is an ongoing non-disclosure obligation at the time the TR was issued.

[74] Twitter reports the % of US legal processes requests that have been issued through MLAT procedures. For example, in H1 2019, 20% of court orders and 3% of search warrants received were explicitly identified as having been issued as a result of MLAT requests, which originated in Argentina, Australia, Belarus, Chile, Finland, India, Monaco, Netherlands, South Korea and Switzerland.

[75] The total number of requests also include informal non-government requests.

[76] Not available

[77] "Information produced (all)" refers to situations where the Wikimedia Foundation provided all of the nonpublic user information requested in the requester's initial message. "Information produced (partial)" refers to situations in which the Wikimedia Foundation provided some nonpublic user information, but less than what was requested in the requester's initial message. For example, this may happen when some of the information requested is information that the Wikimedia Foundation does not collect or store, when the requester asked for information that has already been deleted from the Wikimedia Foundation's systems, or if the requester served the Wikimedia Foundation with valid legal process regarding some, but not all, of the information they wanted.